SOPHOS

Sophos Anti-Virus für Linux, Version 7
Benutzerhandbuch

Stand: Mai 2010

Über dieses Handbuch

Dieses Handbuch erläutert die Verwendung von Sophos Anti-Virus für Linux sowie die Konfiguration der

- Viren-/Spyware-Überprüfung
- Viren-/Spyware-Alarme
- Bereinigung
- Protokolle
- Updates

Das Benutzerhandbuch hilft auch bei der Lösung gängiger Probleme.

Wenn Sie Sophos Anti-Virus auf einzelnen Linux-Computern und Linux-Computern im Netzwerk installieren, aktualisieren oder deinstallieren möchten, nehmen Sie die *Sophos Anti-Virus für Linux, Version 7, Startup-Anleitung* zu Hilfe.

Wenn Sie Sophos Anti-Virus in einem gemischten Linux- und Windows-Netzwerk installieren oder Sophos Anti-Virus zentral über Sophos Enterprise Console verwalten möchten, nehmen Sie die *Sophos Endpoint Security and Control Erweiterte Startup-Anleitung* zu Hilfe.

Sophos Dokumentationen werden unter www.sophos.de/support/docs/ und auf den Sophos CDs veröffentlicht.

Inhalt

In diesem Handbuch verwendete Konventionen 5

Verwendung von Sophos Anti-Virus

1 Über Sophos Anti-Virus für Linux 8

2 Durchführen der On-Access-Überprüfung 11

3 Durchführen der On-Demand-Überprüfung 14

4 Was passiert, wenn Viren/Spyware entdeckt werden? 17

5 Bereinigen von Viren/Spyware 19

6 Ansehen der Protokolle 23

Konfiguration von Sophos Anti-Virus

7 Überblick über die Konfiguration 26

8 Konfiguration der On-Access-Überprüfung 33

9 Konfiguration der On-Demand-Überprüfung 43

10 Konfiguration von Alarmen 54

11 Konfiguration des Sophos Anti-Virus-Protokolls 64

12 Konfiguration der Sophos Anti-Virus GUI 65

Aktualisierung von Sophos Anti-Virus

13 Sofortige Aktualisierung von Sophos Anti-Virus 68

14 Kernel-Support 69

15 Konfiguration der Updates 70

Fehlersuche

16 Fehlersuche 78

Glossar und Index

Glossar 84

Index 88

Technischer Support 90

Copyright 91

In diesem Handbuch verwendete Konventionen

Wenn die Befehlszeile mehr als eine Zeile umfasst, werden die nachfolgenden Zeilen eingerückt angezeigt, beispielsweise:

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesLike
  /home/fred/Report.txt
```

Sie sollten den gesamten Text ohne Zeilenumbruch eingeben.

Verwendung von Sophos Anti-Virus

Über Sophos Anti-Virus für Linux

Durchführen der On-Access-Überprüfung

Durchführen der On-Demand-Überprüfung

Was passiert, wenn Viren/Spyware entdeckt werden?

Bereinigen von Viren/Spyware

Ansehen der Protokolle

1 Über Sophos Anti-Virus für Linux

Mit Sophos Anti-Virus für Linux können Sie Ihr Netzwerk vor Viren/Spyware schützen.

1.1 Benutzeroberflächen

Sophos Anti-Virus hat:

- eine Befehlszeilen-Benutzeroberfläche
- eine grafische Benutzeroberfläche (GUI)

Über die Befehlszeile haben Sie Zugriff auf *alle* Funktionen von Sophos Anti-Virus und können *sämtliche* Arten der Konfiguration durchführen. Die Verwendung und Konfiguration der On-Demand-Überprüfung und -Aktualisierung ist nur über die Befehlszeile möglich.

Sie müssen über Root-Rechte verfügen, um alle Sophos Anti-Virus-Befehle außer savscan, der zur On-Demand-Überprüfung verwendet wird, benutzen zu können.

Dieses Handbuch geht davon aus, dass Sie Sophos Anti-Virus in dem standardmäßigen Speicherort gespeichert haben. Aus diesem Grund basieren die Pfade der beschriebenen Befehle auf diesem Speicherort.

Die Sophos Anti-Virus GUI ermöglicht:

- Prüfung des Status der On-Access-Überprüfung
- Start und Beenden der On-Access-Überprüfung
- Konfiguration der Archivüberprüfung
- Konfiguration dessen, was von der Überprüfung ausgeschlossen wird
- Konfiguration von Alarmen
- Ansehen der Sophos Anti-Virus-Protokolle
- Konfiguration der Bereinigung

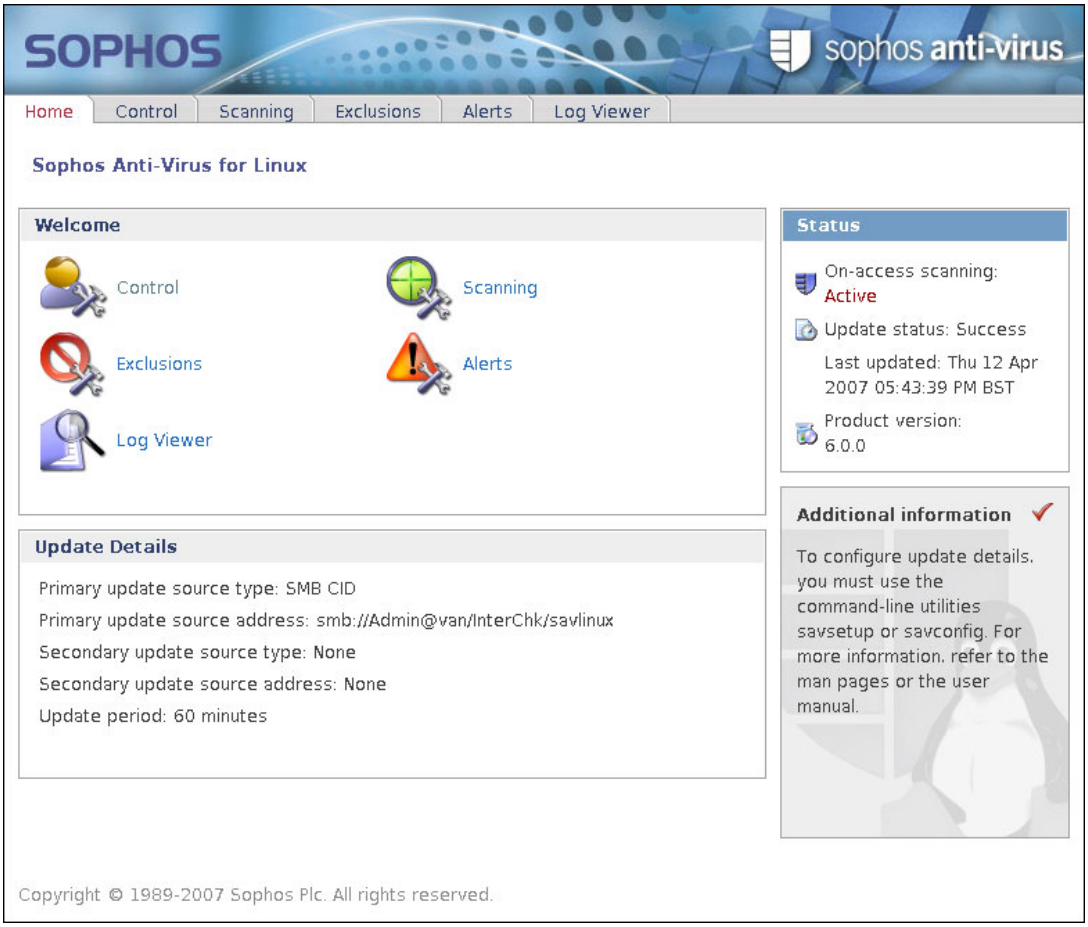
Auch wenn die GUI von dem Root-Benutzer (oder einem anderen Benutzer) ausgeführt werden kann, funktioniert sie nicht mit Root-Rechten. Deshalb kann die GUI nicht auf alle Dateien des Computers zugreifen.

Um die GUI zu verwenden, öffnen Sie einen Browser. In dem Adressfeld geben Sie Folgendes ein:

```
http://localhost:8081
```

Wenn Sie in der Adresse einen anderen http-Port verwenden möchten, konfigurieren Sie die GUI wie in Abschnitt 12 beschrieben.

Der Browser zeigt die Homepage der GUI an.



Wenn Sie zu einer anderen Seite gehen, fragt Sie der Browser nach Zugangsdaten, damit Sie die GUI zur Konfiguration von Sophos Anti-Virus verwenden können.

Um Ihren Benutzernamen zu erfahren, fragen Sie entweder Ihren Systemadministrator oder geben Sie in der Befehlszeile Folgendes ein:

```
/opt/sophos-av/bin/savconfig query HttpUsername
```

Um Ihr Kennwort zu erfahren, fragen Sie entweder Ihren Systemadministrator.

Zur Änderung Ihrer Zugangsdaten siehe Abschnitt 12.

1.2 Überprüfungsarten

Sophos Anti-Virus verfügt über zwei Überprüfungsarten:

- On-Access
- On-Demand

On-Access-Überprüfung fängt Dateien ab, wenn auf sie zugegriffen wird und gestattet Zugriff auf solche, die keine Bedrohung für Ihr Netzwerk darstellen.

Eine **On-Demand-Überprüfung** ist eine Überprüfung des gesamten oder eines Teils des Computers auf Viren/Spyware, die sofort oder zu einem späteren Zeitpunkt durchgeführt werden kann.

1.3 Integration mit Management-Konsole

Sophos Anti-Virus ist in Sophos Enterprise Console integriert, die auf Windows eingesetzt wird und mit der Netzwerkadministratoren Sophos Anti-Virus zentral auf Endpoints verwalten können.

2 Durchführen der On-Access-Überprüfung

On-Access-Überprüfung fängt Dateien ab, wenn auf sie zugegriffen wird und gestattet Zugriff auf solche, die keine Bedrohung für Ihr Netzwerk darstellen.

Dieser Abschnitt beschreibt die *Verwendung* der On-Access-Überprüfung. Die *Konfiguration* wird in Abschnitt 8 beschrieben.

2.1 Überprüfen, ob die On-Access-Überprüfung durchgeführt wird

Befehlszeile

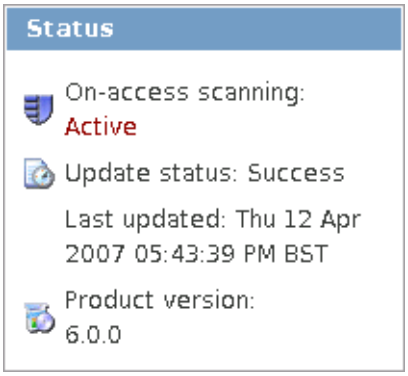
Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savdstatus
```

Sophos Anti-Virus zeigt den Stand der On-Access-Überprüfung an.

GUI

Auf jeder Seite des **Status**-Fensters wird der Stand der On-Access-Überprüfung angezeigt.



2.2 Überprüfen, ob die On-Access-Überprüfung beim Systemstart automatisch durchgeführt wird

Befehlszeile

Wenn Sie über Root-Rechte verfügen, geben Sie Folgendes ein:

```
chkconfig --list
```

Dieser Befehl funktioniert auf TurboLinux eventuell nicht.

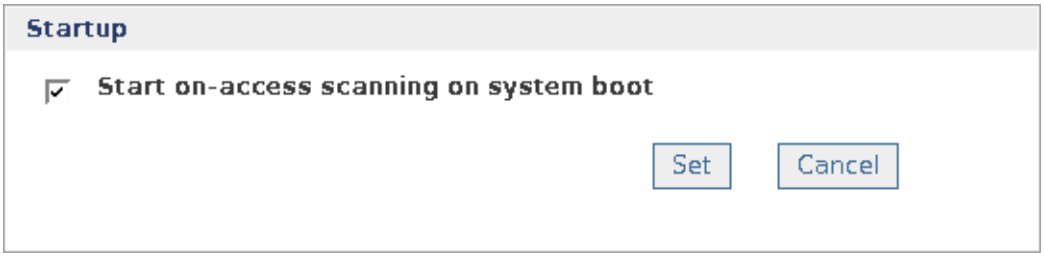
Wenn die Liste einen Eintrag für sav-protect mit 2:on, 3:on, 4:on und 5:on enthält, so wird die On-Access-Überprüfung beim Systemstart automatisch ausgeführt.

Um die On-Access-Überprüfung ansonsten beim Systemstart automatisch auszuführen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savdctl enableOnBoot savd
```

GUI

Prüfen Sie auf der **Control**-Seite im **Startup**-Fenster, ob das Kontrollkästchen **Start on-access scanning on system boot** aktiviert ist. Ist dies nicht der Fall, so aktivieren Sie es, so dass die On-Access-Überprüfung beim Systemstart automatisch ausgeführt wird. Klicken Sie auf **Set**, um die Änderung umzusetzen.



2.3 Starten der On-Access-Überprüfung

Befehlszeile

Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savdctl enable
```

GUI

Auf der **Control**-Seite klicken Sie im **Control**-Fenster auf **Enable On-access Scanning**.

2.4 Beenden der On-Access-Überprüfung

Befehlszeile

Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savdctl disable
```

GUI

Auf der **Control**-Seite klicken Sie im **Control**-Fenster auf **Disable On-access Scanning**.

3 Durchführen der On-Demand-Überprüfung

Eine **On-Demand-Überprüfung** ist eine Überprüfung des gesamten oder eines Teils des Computers auf Viren/Spyware, die sofort oder zu einem späteren Zeitpunkt durchgeführt werden kann.

Als Standard überprüft Sophos Anti-Virus

- Ausführbare Dateien
- .sh- und .pl-Dateien
- Dateien eines Typs, der von Makroviren infiziert werden kann
- HTML-Dateien
- Mit gzip und bzip2 komprimierte Dateien
- Verzeichnisse unter dem angegebenen Verzeichnis
- Objekte, auf die über Symbolic Links verwiesen wird

Um eine vollständige Liste der überprüften Dateiarten zu erhalten, geben Sie Folgendes ein:

```
savscan -vv
```

Informationen über die Änderung dieser Einstellungen finden Sie in Abschnitt 9.

3.1 Überprüfen des Computers

Um den Computer zu überprüfen, geben Sie Folgendes ein:

```
savscan /
```

3.2 Überprüfung eines bestimmten Verzeichnisses oder einer bestimmten Datei

Um ein bestimmtes Verzeichnis oder eine bestimmte Datei zu überprüfen, verwenden Sie den Pfad des Objekts, das überprüft werden soll, z.B.:

```
savscan /usr/mydirectory/myfile
```

3.3 Überprüfung eines Dateisystems

Um ein Dateisystem zu überprüfen, verwenden Sie den Namen des Dateisystems, z.B.:

```
savscan /home
```

In der Befehlszeile kann mehr als ein Dateisystem eingegeben werden.

3.4 Überprüfung eines Bootsektors

Sie können die Bootsektoren auf logischen und physischen Laufwerken überprüfen.

Um Bootsektoren zu überprüfen, melden Sie sich als Superuser an (für ausreichende Zugriffsrechte für die Laufwerksgeräte) und verwenden dann einen der nachfolgend erläuterten Befehle.

Um die Bootsektoren eines bestimmten logischen Laufwerks zu überprüfen, geben Sie Folgendes ein:

```
savscan -bs=XXX, XXX, ...
```

wobei xxx der Name eines Laufwerks ist (z.B. /dev/fd0 oder /dev/hda1).

Um die Bootsektoren aller logischen Laufwerke zu überprüfen, die Sophos Anti-Virus erkennt, geben Sie Folgendes ein:

```
savscan -bs
```

Um die Master Boot-Records aller physischen Laufwerke auf dem Computer zu überprüfen, geben Sie Folgendes ein:

```
savscan -mbr
```

3.5 Festsetzen von Überprüfungszeiten

Sophos Anti-Virus kann den Computer zu festgelegten Zeiten automatisch überprüfen. Nähere Informationen entnehmen Sie bitte dem Anhang.

3.6 Fehlercodes

savscan gibt Fehlercodes aus, wenn ein Fehler auftritt oder wenn Viren oder Spyware entdeckt werden.

0 Wenn keine Fehler aufgetreten sind und keine Viren/Spyware entdeckt wurden.

1 Wenn der Benutzer das Ausführen durch 'Strg + c' unterbricht.

2 Wenn ein Fehler entdeckt wurde, der die weitere Ausführung verhindert.

3 Wenn Viren/Spyware oder Virenfragmente entdeckt wurden.

3.6.1 Erweiterte Fehlercodes

Wenn der savscan-Befehl mit der Option -eec ausgeführt wird, werden andere Fehlercodes ausgegeben.

0 Wenn keine Fehler aufgetreten sind und keine Viren/Spyware entdeckt wurden.

8 Wenn keine schwerwiegenden Fehler aufgetreten sind.

16 Wenn durch Kennwörter geschützte Dateien gefunden wurden. (Sie werden nicht überprüft.)

20 Wenn Viren/Spyware gefunden und desinfiziert wurden.

24 Wenn Viren/Spyware gefunden und nicht desinfiziert wurden.

28 Wenn Viren/Spyware im Speicher gefunden wurden.

32 Wenn ein Fehler bei der Integritätsüberprüfung aufgetreten ist.

36 Wenn schwerwiegende Fehler aufgetreten sind.

40 Wenn die Ausführung unterbrochen wurde.

4 Was passiert, wenn Viren/Spyware entdeckt werden?

4.1 Wenn Viren/Spyware während der On-Access-Überprüfung entdeckt werden

Wenn Sophos Anti-Virus während einer On-Access-Überprüfung einen Virus oder Spyware findet, sperrt es den Zugriff auf die Datei und zeigt eine Meldung, wie unten dargestellt, an.

Sophos Anti-Virus Alert
sophos anti-virus
Virus "EICAR-AV-Test" detected in file "/root/Desktop/eicar.com".
Access to the file has been denied.
Please contact your IT department.
OK

Kann die Meldung nicht angezeigt werden, erscheint die Warnung in der Befehlszeile.

Sophos Anti-Virus protokolliert außerdem das Ereignis im Sophos Anti-Virus Protokoll und sendet einen Alarm an Enterprise Console, wenn der Computer darüber verwaltet wird.

Siehe Abschnitt 5 für Informationen über das Bereinigen von Viren/Spyware.

4.2 Wenn Viren/Spyware bei der On-Demand-Überprüfung entdeckt werden

Wenn Sophos Anti-Virus einen Virus oder Spyware entdeckt, wird dies in der Zeile, die mit >>> beginnt, gefolgt von entweder 'Virus' oder 'Virus Fragment', gemeldet:

```
SAVScan virus detection utility
Version X.XX.XX [Linux/Intel]
Virus data version X.XX, November 2009
Includes detection for 1132356 viruses, trojans and worms
Copyright (c) 1989-2009 Sophos Plc, www.sophos.com

System time 17:24:27, System date 27 November 2009

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src

33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com, email support@sophos.com
End of Scan.
```

Sophos Anti-Virus erfasst dieses Ereignis außerdem im Sophos Anti-Virus Protokoll.

Siehe Abschnitt 5 für Informationen über das Bereinigen von Viren/Spyware.

5 Bereinigen von Viren/Spyware

5.1 Informationen zum Entfernen

Werden Viren/Spyware gefunden, so finden Sie auf der Sophos Website Informationen und Hinweise zur Bereinigung. Gehen Sie zur Threat-Analysen-Seite (www.sophos.de/security/analyses). Suchen Sie nach dem Namen des Virus oder der Spyware, unter dem Sophos Anti-Virus den Virus bzw. die Spyware gemeldet hat.

5.2 Quarantäne für infizierte Dateien

Sie können Sophos Anti-Virus so konfigurieren, dass infizierte Dateien in Quarantäne verschoben werden (beispielsweise um den Zugriff auf diese Dateien zu verhindern). Dies geschieht, indem Besitzer und Rechte für diese Datei geändert werden.

Um das Verschieben in Quarantäne festzulegen, geben Sie Folgendes ein:

```
savscan PATH --quarantine
```

dabei ist PATH der zu überprüfende Pfad.

Als Standardvorgabe ändert Sophos Anti-Virus den Besitzer der infizierten Datei auf den Benutzer, der Sophos Anti-Virus gestartet hat, und die Dateirechte zu -r-------- (0400).

Sie können auch den Benutzer- oder Gruppenbesitzer und die Dateirechte festlegen, so dass Sophos sie für infizierte Dateien anwendet. Dies geschieht mithilfe der Parameter:

```
uid=NNN
user=USERNAME
gid=NNN
group=GROUP-NAME
mode=PPP
```

Sie können nicht mehr als einen Parameter jedes Typs angeben, d.h., Sie können nicht zweimal denselben Benutzernamen oder eine uid und einen Benutzernamen angeben.

Für jeden Parameter, den Sie nicht setzen, werden die Standard-einstellungen angewendet (wie unten angegeben).

Zum Beispiel:

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

Hier wird der Besitzer der infizierten Datei zu virus, der Gruppenbesitzer zu virus und die Dateirechte werden zu -r-------- geändert. Das bedeutet, dass sich die Datei im Besitz des Benutzers virus und Gruppenvirus befindet, aber *nur* der Benutzer virus kann auf die Datei zugreifen (er hat nur Leserechte). Die Datei kann von keinem anderen Benutzer bearbeitet werden (ausgenommen von root).

Wenn Sie die Desinfektion (siehe Abschnitt 5.3) sowie die Quarantäne spezifizieren, versucht Sophos Anti-Virus, infizierte Objekte zu desinfizieren und stellt sie nur dann unter Quarantäne, wenn die Desinfektion fehlschlägt.

5.3 Einstellen der automatischen Bereinigung bei der On-Demand-Überprüfung

Sophos Anti-Virus kann infizierte Daten während der On-Demand-Überprüfung automatisch desinfizieren oder löschen. Alle Vorgänge, die Sophos Anti-Virus hinsichtlich der infizierten Daten durchführt, werden in der Überprüfungs-Übersicht aufgeführt und im Sophos Anti-Virus-Protokoll gespeichert. Standardmäßig ist die automatische Bereinigung deaktiviert.

Die verwendete Methode hängt davon ab, ob Sie eine Datei oder einen Boot-Sektor bereinigen wollen.

5.3.1 Bereinigen von Dateien

Um eine bestimmte Datei zu desinfizieren, geben Sie Folgendes ein:

```
savscan FILE-PATH -di
```

Um alle Dateien auf dem Computer zu desinfizieren, geben Sie Folgendes ein:

```
savscan / -di
```

In beiden Fällen fragt Sophos Anti-Virus nach einer Bestätigung für die Desinfektion.

Durch die Desinfektion der Dokumente werden von dem Virus in dem Dokument vorgenommene Änderungen nicht rückgängig gemacht. (In Abschnitt 5.1 wird erläutert, wie Sie auf der Sophos Website Einzelheiten zu den Nebeneffekten von Viren finden.)

Um eine bestimmte, infizierte Datei zu löschen, geben Sie Folgendes ein:

```
savscan FILE-PATH -remove
```

Um alle infizierten Dateien auf dem Computer zu löschen, geben Sie Folgendes ein:

```
savscan / -remove
```

In beiden Fällen fragt Sophos Anti-Virus nach einer Bestätigung für den Löschvorgang.

5.3.2 Desinfizieren eines Bootsektors

Um einen Bootsektor zu desinfizieren, geben Sie Folgendes ein:

```
savscan -bs=XXX -di
```

wobei `xxx` der Name eines Laufwerks ist.

Um beispielsweise einen Virus von einer Diskette zu entfernen, geben Sie Folgendes ein:

```
savscan -bs=/dev/fd0 -di
```

5.4 Wiederherstellen nach Nebeneffekten

Das Wiederherstellen nach einer Vireninfektion hängt davon ab, wie schwer der Virus den Computer infiziert hat. Einige Viren haben keine Nebeneffekte und andere können so starke Nebeneffekte haben, dass Sie Ihre Festplatte wiederherstellen müssen.

Einige Viren verändern Daten nach und nach. Es ist manchmal schwierig, diese Art der Beschädigung zu erkennen. Aus diesem Grund ist es äußerst wichtig, dass Sie die Virenanalyse auf der Sophos Website lesen und Ihre Dokumente nach der Desinfektion sorgfältig prüfen.

Verlässliche Backups sind äußerst wichtig. Wenn Sie vor der Infektion keine Backups hatten, erstellen Sie sie bitte, um für zukünftige Infektionen gerüstet zu sein.

Mitunter können Sie Daten auch von einer Diskette, die durch einen Virus beschädigt wurde, wiederherstellen. Sophos kann Dienstprogramme zur Verfügung stellen, um einige, von Viren verursachte Schäden zu reparieren. Für weitere Einzelheiten wenden Sie sich an den technischen Support von Sophos.

6 Ansehen der Protokolle

Sophos Anti-Virus führt Details der Überprüfung in dem Sophos Anti-Virus-Protokoll und syslog-Protokoll auf. Zudem werden Viren-/Spyware- und Fehlerereignisse in dem Sophos Anti-Virus-Protokoll gespeichert. Meldungen in dem Sophos Anti-Virus-Protokoll werden in die Sprachen übersetzt, die das Produkt unterstützt.

Befehlszeile

Verwenden Sie den Befehl savlog. Es können verschiedene Varianten des Befehls verwendet werden, um das Ergebnis auf bestimmte Meldungen zu beschränken und die Anzeige zu steuern. Um alle Meldungen, die in den letzten 24 Stunden in dem Sophos Anti-Virus-Protokoll aufgeführt wurden, einschließlich Datum und Zeit im UTC/ISO 8601-Format anzuzeigen, geben Sie Folgendes ein:

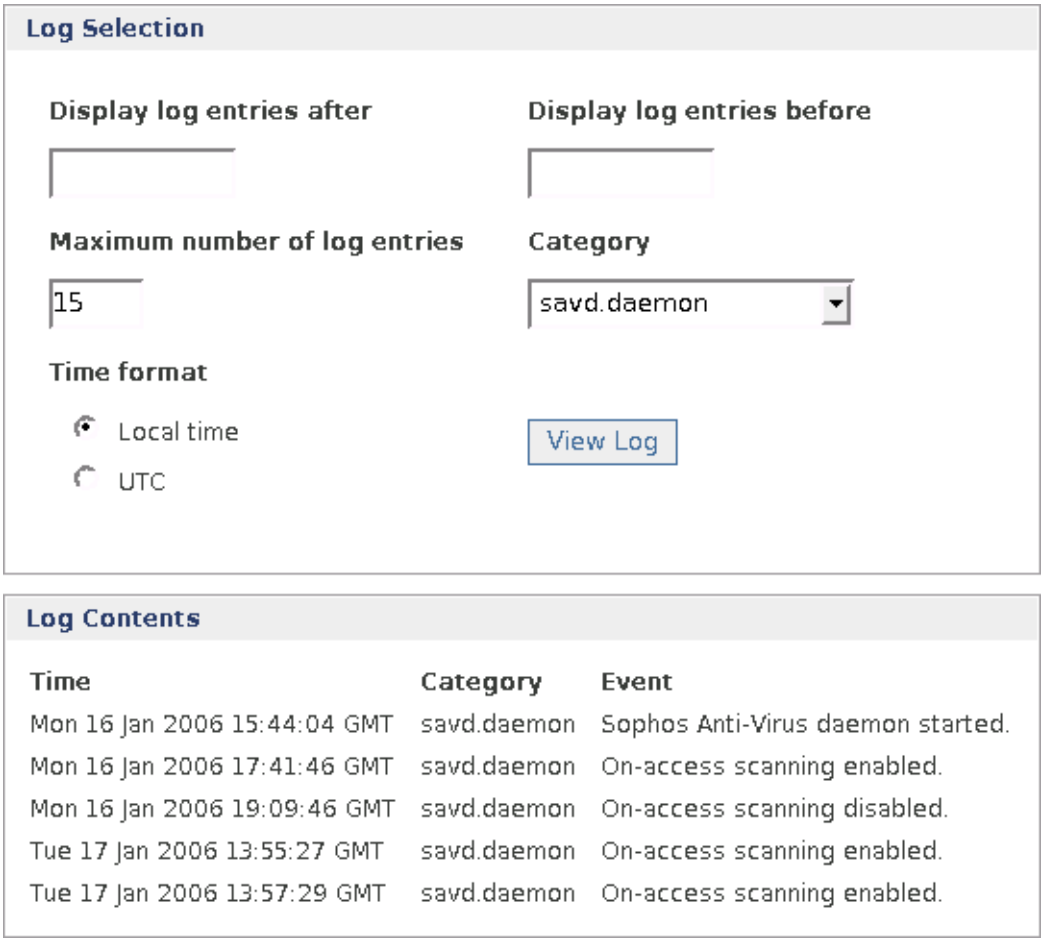
```
/opt/sophos-av/bin/savlog --today --utc
```

Um eine vollständige Liste der Optionen anzusehen, die mit savlog verwendet werden können, geben Sie Folgendes ein:

```
man savlog
```

GUI

Gehen Sie auf die Seite **Log Viewer**.



Mithilfe der Textfelder und Schaltflächen im Fenster **Log Selection** legen Sie fest, welche Meldungen angezeigt werden sollen. Klicken Sie dann auf **View Log**, um die Meldungen in dem Fenster **Log Contents** anzuzeigen.

Konfiguration von Sophos Anti-Virus

Überblick über die Konfiguration

Konfiguration der On-Access-Überprüfung

Konfiguration der On-Demand-Überprüfung

Konfiguration von Alarmen

Konfiguration der Sophos Anti-Virus-Protokolle

Konfiguration der Sophos Anti-Virus GUI

7 Überblick über die Konfiguration

Dieser Abschnitt trifft für alle Konfigurationen zu, mit Ausnahme der für On-Demand-Überprüfungen, die in Abschnitt 9 beschrieben wird. Die Verwendung von Sophos Enterprise Console oder der Befehle savconfig und savsetup hat keine Auswirkungen auf die On-Demand-Überprüfung.

7.1 Konsolen-basierte Konfiguration von Sophos Anti-Virus in einem Netzwerk

Sie können Sophos Anti-Virus, *Version 7*, auf Endpoints mit Enterprise Console, die auf Windows eingesetzt wird, verwalten. Sie können damit die meisten Konfigurationen über eine benutzerfreundliche GUI durchführen. Die Installation der Konsole wird in der *Erweiterten Startup-Anleitung zu Sophos Endpoint Security and Control* beschrieben, die unter www.sophos.de/support/docs und den Sophos CDs zur Verfügung steht.

Weitere Informationen zum Gebrauch der Konsole zur Konfiguration von Sophos Anti-Virus finden Sie in der Konsolenhilfe. Wenn Sie die Konsole verwenden, trifft Folgendes für die Konfiguration zu:

- Parameter, die nicht mithilfe der Konsole eingestellt werden können, können lokal auf jedem Endpoint mit savconfig (Abschnitt 7.4) eingestellt werden. Diese Parameter werden von der Konsole ignoriert.
- Automatische Updates können nur über die Konsole konfiguriert werden. Sie können nicht am Endpoint konfiguriert werden.

Sophos unterstützt die gemeinsame Verwendung von Konsole- und CID-basierten Konfigurationen nicht, die zuvor Unternehmenskonfiguration genannt wurden. Wenn Sie eine CID-basierte Konfiguration mit *Version 5* von Sophos Anti-Virus verwendet haben, müssen Sie wählen, ob Sie weiterhin diese Konfiguration oder stattdessen Enterprise Console verwenden möchten. Wenn Sie Enterprise Console verwenden möchten, lesen Sie bitte den Sophos Support Knowledgebase Artikel 22297 (www.sophos.de/support/knowledgebase/article/22297.html).

7.2 CID-basierte Konfiguration von Sophos Anti-Virus in einem Netzwerk

Eine CID (zentrales Installationsverzeichnis)-basierte Konfiguration, zuvor Unternehmenskonfiguration genannt, erfordert keinen Windows-Computer. Sie umfasst das Ändern einer Konfigurationsdatei, die in dem CID gespeichert ist, indem die Einträge von Parametern mit dem Befehl savconfig eingestellt werden (Abschnitt 7.4). Wenn Endpoints sich dann über das CID aktualisieren, verwenden sie diese Konfiguration. Sie können Parameter außerdem sperren, damit sie auf Endpoints nicht verändert werden können. Auf diese Weise können Sie die Konfiguration von Sophos Anti-Virus an jedem Endpoint festlegen, ohne dass die Einstellungen von einem Endpoint-Benutzer verändert werden können.

Es gibt zwei Konfigurationsdateien: die *aktive* Konfigurationsdatei im CID und die *nicht aktive* Konfigurationsdatei, die an anderer Stelle gespeichert wird. Wenn Sie die aktive Datei ändern wollen, müssen Sie die nicht aktive Datei ändern und ein Programm verwenden, um die aktive Datei durch die nicht aktive Datei zu ersetzen.

7.2.1 *Erstellung* der aktiven Konfigurationsdatei im CID

1. Erstellen Sie die nicht aktive Konfigurationsdatei in einem Verzeichnis Ihrer Wahl, jedoch nicht im CID. Sie müssen den Befehl savconfig verwenden und Folgendes angeben:

   - Den Namen der nicht aktiven Datei, einschließlich der Dateierweiterung cfg
   - Dass Sie auf die *Unternehmens*-Ebene der Datei zugreifen (für weitere Informationen zu Ebenen, siehe Abschnitt 7.2.3)
   - Die Einstellung eines Parameters

   Verwenden Sie die folgende Syntax:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c PARAMETER VALUE
   ```

   dabei ist CONFIG-FILE der Pfad der nicht aktiven Datei, -c weist darauf hin, dass Sie auf die Unternehmensebene zugreifen wollen, PARAMETER ist der Parameter, den Sie einstellen möchten und VALUE ist der Eintrag, auf den Sie den Parameter einstellen möchten. Um beispielsweise eine Datei namens CIDconfig.cfg zu erstellen und eine On-Access-Überprüfung zu starten, wenn der Sophos Anti-Virus-Dämon gestartet wird, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c EnableOnStart
     Enabled
   ```

   Einzelheiten zur Verwendung von savconfig sind in Abschnitt 7.4 zu finden.

2. Wenn erforderlich, legen Sie andere Parameter mithilfe des Befehls savconfig fest. Sie müssen den Namen der Offline-Datei angeben und, dass Sie auf die Unternehmensebene zugreifen, siehe oben.

3. Um die Einstellungen von Parametern zu sehen, verwenden Sie den Anfrage-Vorgang (Query Operation). Sie können entweder die Einstellungen eines einzelnen oder aller Parameter ansehen. Um beispielsweise die Einstellungen aller von Ihnen festgelegten Parametern anzusehen, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c query
   ```

4. Wenn Sie die Parameter eingestellt haben, starten Sie das addcfg-Dienstprogramm, um die Konfiguration in das CID zu kopieren, so dass die Endpoints sie von dort herunterladen können, wenn sie die nächste Aktualisierung durchführen. Das Dienstprogramm befindet sich im CID. Je nachdem, wo sich das CID befindet, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
   ```

   dabei bezeichnet CONFIG-FILE den Pfad der nicht aktiven Datei.

7.2.2 *Update* der aktiven Konfigurationsdatei im CID

1. Aktualisieren Sie die nicht aktive Konfigurationsdatei. Sie müssen den Befehl savconfig verwenden und Folgendes angeben:

   - Name der Offline-Datei
   - Dass Sie auf die *Unternehmens*-Ebene der Datei zugreifen (für weitere Informationen zu Ebenen, siehe Abschnitt 7.2.3)
   - Die Einstellung eines Parameters

   Verwenden Sie die folgende Syntax:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c PARAMETER VALUE
   ```

   dabei ist CONFIG-FILE der Pfad der Offline-Datei, -c weist darauf hin, dass Sie auf die Unternehmensebene zugreifen wollen, PARAMETER ist der Parameter, den Sie einstellen möchten und VALUE ist der Eintrag, auf den Sie den Parameter einstellen möchten. Um beispielsweise eine Datei namens CIDconfig.cfg zu aktualisieren und eine On-Access-Überprüfung zu starten, wenn der Sophos Anti-Virus-Dämon gestartet wird, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c EnableOnStart
     Enabled
   ```

   Für Einzelheiten zur Verwendung von savconfig, siehe Abschnitt 7.4.

2. Wenn erforderlich, legen Sie andere Parameter mithilfe des Befehls savconfig fest. Sie müssen den Namen der nicht aktiven Datei angeben und, dass Sie auf die Unternehmensebene zugreifen, siehe oben.

3. Um die Einstellungen von Parametern zu sehen, verwenden Sie den Anfrage-Vorgang (Query Operation). Sie können entweder die Einstellungen eines einzelnen oder aller Parameter ansehen. Um beispielsweise die Einstellungen aller von Ihnen festgelegten Parameter anzusehen, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CIDconfig.cfg -c query
   ```

4. Wenn Sie die Parameter eingestellt haben, starten Sie das addcfg-Dienstprogramm, um die Konfiguration in das CID zu kopieren, so dass die Endpoints sie von dort herunterladen können, wenn sie die nächste Aktualisierung durchführen. Das Dienstprogramm befindet sich im CID. Je nachdem, wo sich das CID befindet, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/update/cache/Primary/addcfg.sh -fCONFIG-FILE
   ```

   dabei bezeichnet CONFIG-FILE den Pfad der nicht aktiven Datei.

7.2.3 Konfigurationsebenen

Jede Installation von Sophos Anti-Virus umfasst eine lokale Konfigurationsdatei, die die Einstellungen für alle Bereiche von Sophos Anti-Virus enthält.

Jede lokale Konfigurationsdatei enthält eine Anzahl an *Ebenen*:

- Sophos: Diese Ebene ist stets in der Datei enthalten. Sie enthält die Ausgangseinstellungen, die nur von Sophos geändert werden.
- Unternehmen (Corporate): Diese Ebene ist verfügbar, wenn die Installation von dem zentralen Installationsverzeichnis (CID) aus geschieht, wie in den Abschnitten 7.2.1 und 7.2.2 beschrieben.
- Benutzer (User): Diese Ebene ist verfügbar, wenn eine lokale Konfiguration durchgeführt wird. Dazu gehören Einstellungen, die sich nur auf die Installation auf diesem Computer beziehen.

Jede Ebene verwendet dieselben Parameter, so dass dieselben Parameter in mehreren Ebenen eingestellt werden können. Wenn Sophos Anti-Virus jedoch den Eintrag eines Parameters prüft, geschieht das gemäß der Prioritätenordnung der Ebenen:

- Standardmäßig hat die Unternehmensebene Priorität über die Benutzerebene.
- Die Unternehmens- und Benutzerebenen haben Priorität über die Sophos-Ebene.

Wenn ein Parameter beispielsweise in der Benutzer- und Unternehmensebene festgelegt wird, so wird der Eintrag in der Unternehmensebene verwendet. Sie können die Einstellung der Einträge in den einzelnen Parametern der Unternehmensebene aber auch ändern, so dass sie keine Priorität mehr haben.

Wenn die lokale Konfigurationsdatei von der Konfigurationsdatei im CID aktualisiert wird, wird die Unternehmensebene in der lokalen Datei durch die der Datei im CID ersetzt.

7.3 Konfiguration von Sophos Anti-Virus auf einem einzelnen Computer

Verwenden Sie den Befehl savconfig, um einen einzelnen Computer zu konfigurieren. Einzelheiten zur Verwendung von savconfig sind in Abschnitt 7.4 zu finden. Standardmäßig wendet savconfig die Konfiguration auf die Benutzerebene der lokalen Konfigurationsdatei an.

7.4 Der Konfigurationsbefehl savconfig

Sophos Anti-Virus wird mithilfe des Befehls savconfig konfiguriert. Der Pfad des Befehls lautet /opt/sophos-av/bin. Die Verwendung dieses Befehls zur Konfiguration bestimmter Funktionen von Sophos Anti-Virus wird im restlichen Teil dieses Handbuchs erklärt. Der Rest dieses Unterabschnitts erklärt die Syntax.

Die Syntax von savconfig lautet:

```
savconfig [OPTION] ... [OPERATION] [PARAMETER] [VALUE] ...
```

Um eine vollständige Liste der Optionen, Vorgänge (Operations) und Parameter zu sehen, geben Sie Folgendes ein:

```
man savconfig
```

Nachstehend wird eine Übersicht gegeben.

7.4.1 OPTION

Sie können eine oder mehrere Optionen festlegen. Die Optionen beziehen sich auf die *Ebenen* in den lokalen Konfigurationsdateien jeder Installation. Informationen zu den Ebenen sind in Abschnitt 7.2.3 zu finden. Standardmäßig bezieht sich der Befehl auf die Benutzerebene. Wenn Sie also beispielsweise auf die Unternehmensebene (Corporate) zugreifen wollen, können Sie die Optionen -c oder --corporate verwenden.

Standardmäßig sind die Einträge (Values) in der Unternehmensebene festgesetzt, so dass sie Priorität über die Einträge der Benutzerebene haben.

Wenn jedoch die Benutzereinstellungen Priorität über die Unternehmenseinstellungen haben sollen, so müssen Sie die Option --nolock verwenden. Um beispielsweise den Eintrag LogMaxSizeMB festzulegen und einzustellen, dass er keine Priorität hat, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c
   LogMaxSizeMB 50
```

Wenn Sie Enterprise Console verwenden, können Sie nur die Einträge der Antiviren-Richtlinien-Parameter mithilfe der Option --consoleav anzeigen. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleav query
```

Sie können auch nur die Einträge der Konsolen-Update-Richtlinie mithilfe der Option --consoleupdate anzeigen. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

7.4.2 OPERATION

Sie können einen Vorgang (Operation) festlegen. Die Vorgänge hängen größtenteils davon ab, auf welche Weise Sie auf die Parameter zugreifen wollen. Einige Parameter verfügen über nur einen Eintrag, während andere über eine Liste an Einträgen verfügen. Aus diesem Grund erlauben die Vorgänge es Ihnen, Einträge zu einer Liste hinzuzufügen oder daraus zu entfernen. Der Parameter CacheFilesystems ist beispielsweise eine *Auflistung* verschiedener Dateisysteme.

Um die Einträge von Parametern anzuzeigen, verwenden Sie die Vorgangsanfrage. Um beispielsweise den Eintrag des ExcludeFileOnGlob-Parameters anzuzeigen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig query ExcludeFileOnGlob
```

Wenn Sie Enterprise Console verwenden und savconfig Parametereinträge ausgibt, werden die mit der relevanten Konsolenrichtlinie nicht übereinstimmenden mit dem Wort 'Conflict' deutlich markiert.

7.4.3 PARAMETER

Sie können einen Parameter festlegen. Um alle grundlegenden Parameter aufzulisten, die festgelegt werden können, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig -v
```

Bei einigen Parametern ist es erforderlich, zusätzliche Parameter ebenfalls festzulegen.

7.4.4 VALUE

Sie können einen oder mehrere Einträge (Values) festlegen, die einem Parameter zugeordnet werden. Wenn Leerzeichen in einem Eintrag enthalten sind, müssen Sie ihn in einfache Anführungszeichen setzen.

7.5 Der Konfigurationsbefehl savsetup

savsetup ist das Dienstprogramm, mit dem Sie die Konfiguration der Updates und der Sophos Anti-Virus GUI einrichten. Obwohl dieses Dienstprogramm Ihnen nur erlaubt, auf einige der Parameter zuzugreifen, auf die Sie mit savconfig zugreifen können, ist seine Verwendung einfacher. Es fragt Sie nach Parametereinträgen und Sie müssen einfach nur die Einträge auswählen oder eingeben. Um savsetup auszuführen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savsetup
```

Wenn Sie savsetup starten, haben Sie die Wahl bei der Konfiguration: Update oder die Sophos Anti-Virus GUI. Geben Sie die entsprechende Nummer ein, um Ihre Auswahl zu treffen. Beantworten Sie dann die angezeigten Fragen.

8 Konfiguration der On-Access-Überprüfung

Wenn Sie einen einzelnen Computer konfigurieren, der sich in einem Netzwerk befindet, so kann solch eine Konfiguration verloren gehen, wenn der Computer eine neue Konsolen-basierte Konfiguration herunterlädt.

8.1 Dateien und Verzeichnisse von der Überprüfung ausschließen

Sie können Dateien und Verzeichnisse auf verschiedene Weise von der Überprüfung ausschließen:

- indem Sie Datei- oder Verzeichnisnamen verwenden (Abschnitt 8.1.1)
- indem Sie Dateitypen verwenden (Abschnitt 8.1.2)
- indem Sie Platzhalter verwenden (Abschnitt 8.1.3)

Wenn Sie Dateien und Verzeichnisse ausschließen möchten, deren Namen nicht mit UTF-8 verschlüsselt sind, siehe Abschnitt 8.1.4.

8.1.1 Verwendung des Datei- oder Verzeichnisnamens

Wenn Sie Enterprise Console verwenden und eine Anti-Viren-Richtlinie haben, die Ausnahmen unter Verwendung des Datei- oder Verzeichnisnamens festlegt, verursachen solche Ausnahmen, die Sie lokal an einem Endpoint einstellen, dass die Konsole den Endpoint als nicht mit der Richtlinie übereinstimmend anzeigt. Der Konsolenbenutzer kann den Endpoint zwingen, mit der Richtlinie übereinzustimmen und folglich die lokal eingestellten Ausnahmen zu verwerfen.

Befehlszeile

Um eine bestimmte Datei oder ein bestimmtes Verzeichnis auszuschließen, verwenden Sie den Parameter ExcludeFilePaths. Um beispielsweise die Datei /tmp/report zur Liste an Dateien und Verzeichnissen, die ausgeschlossen werden sollen, hinzuzufügen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFilePaths /tmp/report
```

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, verwenden Sie den Vorgang 'Entfernen' (Remove Operation). Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report
```

GUI

Um eine bestimmte Datei oder ein bestimmtes Verzeichnis auszuschließen, geben Sie auf der Seite **Exclusion Configuration** im Fenster **File Scanning Exclusions** den Pfad in das Textfeld **Files or directories (with or without wildcards)** ein. Klicken Sie auf **Add New Entry**, um den Pfad zu der Liste hinzuzufügen.

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, wählen Sie es und klicken Sie auf **Remove Selected Entry**.

8.1.2 Verwendung des Dateityps

Wenn Sie auszuschließende Objekte auf diese Art und Weise angeben, ist die Überprüfung weniger effektiv, als wenn sie auszuschließende Objekte anhand des Datei- oder Verzeichnisnamens, des Platzhalters oder anhand von regulären Ausdrücken angeben.

Befehlszeile

Um Dateien auszuschließen, die demselben Dateityp angehören wie die festgelegte Datei, verwenden Sie den Parameter ExcludeFilesLike. Um beispielsweise den Dateityp der Datei Report.txt zur Liste von Dateiausnahmen hinzuzufügen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFilesLike /home/fred/Report.txt
```

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, verwenden Sie den Vorgang 'Entfernen' (Remove Operation). Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesLike
  /home/fred/Report.txt
```

Um Dateien eines bestimmten Dateityps auszuschließen, verwenden Sie den Parameter ExcludeFileOnType. Bei dem Dateityp muss es sich um einen Eintrag handeln, der von dem Dateibefehl verstanden wird. (Um weitere Informationen zu dem Dateibefehl zu erhalten, geben Sie `man file` ein.) Um beispielsweise Dateien des Dateityps ASCII-Text zur Liste auszuschließender Dateitypen hinzuzufügen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFileOnType 'ASCII text'
```

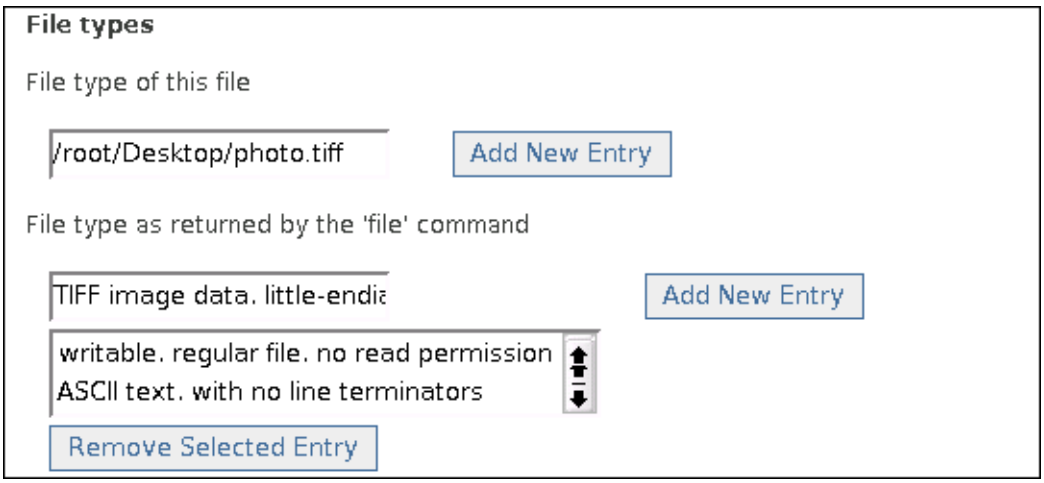
Um ein ausgeschlossenes Objekt von der Liste zu entfernen, verwenden Sie den Vorgang 'Entfernen' (Remove Operation). Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnType 'ASCII text'
```

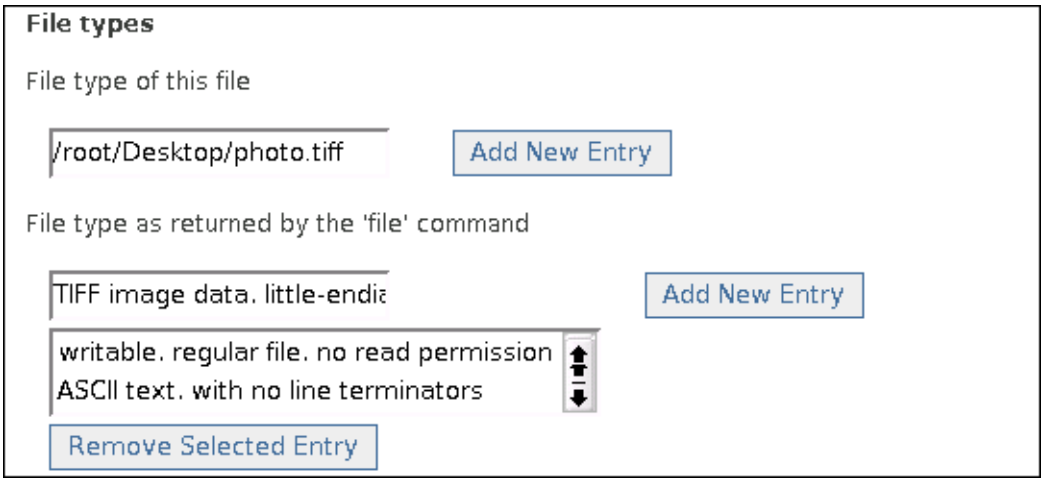
Sophos Anti-Virus nimmt eine teilweise Angleichung der Dateitypen vor. Somit werden alle Dateitypen ausgeschlossen, die dem festgelegten Dateityp bis zu einer Anzahl an Zeichen in dem festgelegten Dateityp, anfangend von links, entsprechen. 'TIFF' schließt beispielsweise alle Typen von TIFF-Dateien aus, aber 'TIFF image data, little-endian' schließt nur einige TIFF-Dateitypen aus.

GUI

Um Dateien auszuschließen, die demselben Dateityp angehören wie die spezifische Datei, geben Sie auf der Seite **Exclusion Configuration** in dem Bereich **File Scanning Exclusions** den Pfad der Datei in dem Textfeld namens **File type of this file** ein. Klicken Sie auf **Add New Entry**, um den Dateityp zur Liste auszuschließender Dateinamen hinzuzufügen.


File types
File type of this file
/root/Desktop/photo.tiff
Add New Entry
File type as returned by the 'file' command
TIFF image data, little-endia
Add New Entry
writable, regular file, no read permission
ASCII text, with no line terminators
Remove Selected Entry

Um Dateien eines bestimmten Dateityps auszuschließen, geben Sie auf der Seite **Exclusion Configuration** im Fenster **File Scanning Exclusions** in dem Textfeld **File type as returned by the 'file' command** den Dateityp ein. (Um weitere Informationen zu dem Dateibefehl zu erhalten, geben Sie `man file` ein.) Klicken Sie auf **Add New Entry**, um den Dateityp zu der Liste hinzuzufügen.


File types
File type of this file
/root/Desktop/photo.tiff
Add New Entry
File type as returned by the 'file' command
TIFF image data, little-endia
Add New Entry
writable, regular file, no read permission
ASCII text, with no line terminators
Remove Selected Entry

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, wählen Sie es und klicken Sie auf **Remove Selected Entry**.

Sophos Anti-Virus nimmt eine teilweise Angleichung der Dateitypen vor. Somit werden alle Dateitypen ausgeschlossen, die dem festgelegten Dateityp bis zu einer Anzahl an Zeichen in dem festgelegten Dateityp, anfangend von links, entsprechen. 'TIFF' schließt beispielsweise alle Typen von TIFF-Dateien aus, aber 'TIFF image data, little-endian' schließt nur einige TIFF-Dateitypen aus.

8.1.3 Verwendung von Platzhaltern

Wenn Sie Enterprise Console verwenden und eine Anti-Viren-Richtlinie haben, die Ausnahmen unter Verwendung von Platzhaltern festlegt, verursachen solche Ausnahmen, die Sie lokal an einem Endpoint einstellen, dass die Konsole den Endpoint als nicht mit der Richtlinie übereinstimmend anzeigt. Der Konsolenbenutzer kann den Endpoint zwingen, mit der Richtlinie übereinzustimmen und folglich die lokal eingestellten Ausnahmen zu verwerfen.

Befehlszeile

Um Dateien und Verzeichnisse mithilfe von Platzhaltern auszuschließen, verwenden Sie den Parameter ExcludeFileOnGlob. Gültige Platzhalter sind '*', das mit einem oder mehreren Zeichen übereinstimmt, und '?', das nur mit einem Zeichen übereinstimmt. Um beispielsweise alle Textdateien des Temp-Verzeichnisses zur Liste auszuschließender Dateien und Verzeichnisse hinzuzufügen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFileOnGlob '/tmp/*.txt'
```

Wenn Sie den Ausdruck nicht mit Anführungszeichen schließen, erweitert Linux den Ausdruck und übergibt die Liste von Dateien an Sophos Anti-Virus. Dies ist zur Ausnahme von Dateien hilfreich, die bereits existieren, und zum Aktiviren von Dateien, die erstellt und später überprüft werden sollen. Um beispielsweise Textdateien zur Liste hinzuzufügen, die bereits im /tmp-Verzeichnis existieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFileOnGlob /tmp/*.txt
```

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, verwenden Sie den Vorgang 'Entfernen' (Remove Operation). Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob
   '/tmp/notes.txt'
```

GUI

Um Dateien und Verzeichnisse durch die Verwendung von Platzhaltern auszuschließen, geben Sie auf der Seite **Exclusion Configuration** im Fenster **File Scanning Exclusions** den Pfad in das Textfeld **Files or directories (with or without wildcards)** ein. Gültige Platzhalter sind '*', das mit einem oder mehreren Zeichen übereinstimmt und '?', das nur mit einem Zeichen übereinstimmt. Klicken Sie auf **Add New Entry**, um den Pfad zu der Liste hinzuzufügen.

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, wählen Sie es und klicken Sie auf **Remove Selected Entry**.

8.1.4 Festlegen der Zeichenverschlüsselung von Verzeichnisnamen und Dateinamen

Mit Linux können Sie Verzeichnisse und Dateien mit beliebiger Zeichenverschlüsselung angeben (z.B. UTF-8, EUC_jp). Sophos Anti-Virus speichert Ausnahmen jedoch nur in UTF-8. Wenn Sie also Verzeichnisse und Dateien von der Überprüfung ausschließen möchten, deren Namen nicht mit UTF-8 verschlüsselt sind, geben Sie die Ausnahmen in UTF-8 und die Verschlüsselungen mit dem Parameter 'ExclusionEncodings' an. Dann werden die Namen aller Verzeichnisse und Dateien, die Sie ausschließen, in jeder der angegebenen Verschlüsselungen getestet und alle übereinstimmenden Verzeichnisse und Dateien ausgeschlossen. Dies trifft für Ausnahmen zu, die mit den Parametern 'ExcludeFilePaths' und 'ExcludeFileOnGlob' angegeben wurden. Standardmäßig werden UTF-8, EUC_jp und ISO-8859-1 (Latin-1) angegeben.

Wenn Sie beispielsweise Verzeichnisse und Dateien ausschließen wollen, deren Namen in EUC_cn verschlüsselt sind, geben Sie die Namen der Verzeichnisse und Dateien mit dem Parameter 'ExcludeFilePaths' und/oder 'ExcludeFileOnGlob' an. Fügen Sie dann EUC_cn zur Liste von Verschlüsselungen hinzu:

```
/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn
```

Danach testet Sophos Anti-Virus alle Verzeichnisnamen und Dateinamen, die Sie angegeben haben, in UTF-8, EUC_jp, ISO-8859-1 (Latin-1) und EUC_cn . Es schließt dann alle Verzeichnisse und Dateien aus, deren Namen übereinstimmen.

8.2 Dateisysteme von der Überprüfung der Dateien ausschließen

Befehlszeile

Um Dateisysteme durch Verwendung von Dateisystem-Typen von der Überprüfung von Dateien auszuschließen, verwenden Sie den Parameter 'ExcludeFilesystems'. Standardmäßig werden keine Dateisystem-Typen ausgeschlossen. Gültige Dateisystem-Typen werden in der Datei /proc/filesystems aufgeführt. Um beispielsweise nfs zur Liste von Dateisystem-Typen hinzuzufügen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig ExcludeFilesystems nfs
```

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, verwenden Sie den Vorgang 'Entfernen' (Remove Operation). Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs
```

GUI

Um Dateisysteme durch die Verwendung von Dateisystem-Typen von der Überprüfung von Dateien auszuschließen, klicken Sie auf der Seite **Exclusion Configuration** im Fenster **File Scanning Exclusions** auf den Pfeil in dem Textfeld mit der Bezeichnung **Filesystem types**. Wählen Sie einen der Dateisystem-Typen aus der Liste aus. Klicken Sie auf **Add New Entry**, um den Dateisystem-Typ zu der Liste hinzuzufügen.

Um ein ausgeschlossenes Objekt von der Liste zu entfernen, wählen Sie es und klicken Sie auf **Remove Selected Entry**.

8.3 Überprüfung von Archiven

Die Überprüfung archivierter Dateien verlangsamt die Überprüfung enorm und ist nur selten erforderlich. Auch wenn Sie diese Option nicht aktivieren, wird die extrahierte Datei überprüft, sobald Sie versuchen, auf eine Datei in einer archivierten Datei zuzugreifen.

Befehlszeile

Um die Überprüfung von Archiven zu aktivieren, geben Sie Folgendes ein:

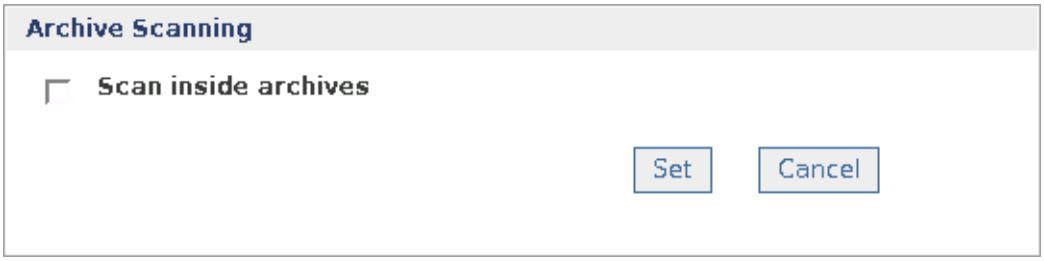
```
/opt/sophos-av/bin/savconfig set ScanArchives enabled
```

Um die Überprüfung von Archiven zu deaktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig set ScanArchives disabled
```

GUI

Um die Überprüfung von Archiven zu konfigurieren, gehen Sie auf die Seite **Scanning Configuration** zum Fenster **Archive Scanning**.



Konfigurieren Sie die Überprüfung von Archiven wie unten beschrieben. Wenn Sie dies getan haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

Um die Überprüfung von Archiven zu aktivieren, wählen Sie das Kontrollkästchen **Scan inside archives** aus.

Um die Überprüfung von Archiven zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Scan inside archives**.

8.4 Einrichten der automatischen Bereinigung

Sophos Anti-Virus kann infizierte Daten während der On-Access-Überprüfung automatisch desinfizieren oder löschen. Alle Vorgänge, die Sophos Anti-Virus hinsichtlich der infizierten Daten durchführt, werden im Sophos Anti-Virus-Protokoll gespeichert. Standardmäßig ist die automatische Bereinigung deaktiviert.

Befehlszeile

Um die automatische Desinfektion von infizierten Dateien und Bootbereichen zu aktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig AutomaticAction disinfect
```

Durch die Desinfektion der Dokumente werden von dem Virus in dem Dokument vorgenommene Änderungen nicht rückgängig gemacht. (In Abschnitt 5.1 wird erläutert, wie Sie auf der Sophos Website Einzelheiten zu den Nebenwirkungen von Viren finden.)

Zur Deaktivierung der automatischen Desinfektion geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect
```

Um das automatische Löschen infizierter Dateien zu aktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig AutomaticAction delete
```

Sie sollten diese Option nur verwenden, wenn Ihnen der technische Support von Sophos dazu geraten hat. Wenn es sich bei der infizierten Datei um eine Mailbox handelt, löscht Sophos Anti-Virus mitunter die gesamte Mailbox.

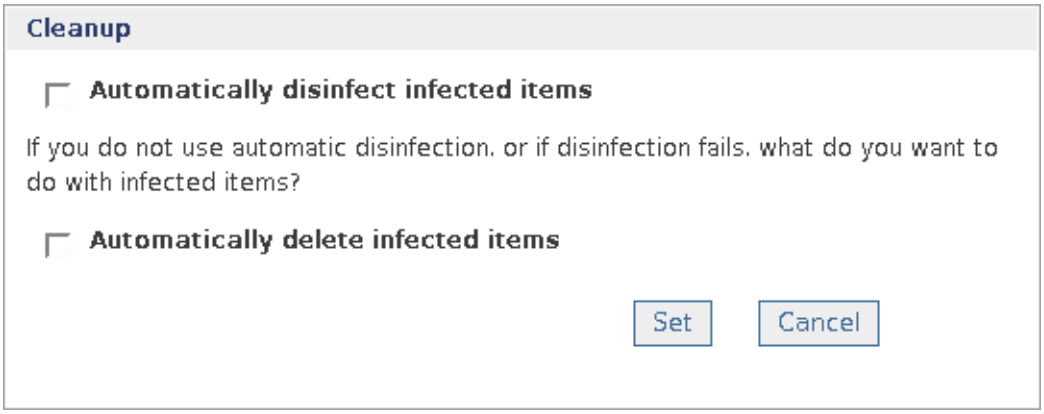
Um das automatische Löschen zu deaktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig remove AutomaticAction delete
```

Sie können sowohl automatisches Löschen als auch Desinfizieren aktiviren, dies wird von Sophos jedoch nicht empfohlen. Wenn Sie dies tun, versucht Sophos Anti-Virus, das Objekt zuerst zu *desinfizieren*. Ist die Desinfektion nicht möglich, wird das Objekt entfernt.

GUI

Um das automatische Entfernen zu aktivieren, gehen Sie zur **Scanning**-Seite in das **Cleanup**-Fenster.


Cleanup
Automatically disinfect infected items
If you do not use automatic disinfection, or if disinfection fails, what do you want to do with infected items?
Automatically delete infected items
Set
Cancel

Konfigurieren Sie das Entfernen wie nachstehend beschrieben. Wenn Sie dies getan haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

Um die automatische Desinfektion infizierter Dateien und Bootbereiche zu aktivieren, klicken Sie das Kontrollkästchen **Automatically disinfect infected items** an. Durch die Desinfektion der Dokumente werden von dem Virus in dem Dokument vorgenommene Änderungen nicht rückgängig gemacht. (In Abschnitt 5.1 wird erläutert, wie Sie auf der Sophos Website Einzelheiten zu den Nebenwirkungen von Viren finden.)

Um das automatische Entfernen von infizierten Dateien zu aktivieren, klicken Sie das Kontrollkästchen **Automatically delete infected items** an.

Sie sollten diese Option nur verwenden, wenn Ihnen der technische Support von Sophos dazu geraten hat. Wenn es sich bei der infizierten Datei um eine Mailbox handelt, löscht Sophos Anti-Virus mitunter die gesamte Mailbox.

Sie können sowohl automatisches Löschen als auch Desinfizieren aktivieren, dies wird von Sophos jedoch nicht empfohlen. Wenn Sie dies tun, versucht Sophos Anti-Virus das Objekt zuerst zu *desinfizieren*. Ist die Desinfektion nicht möglich, wird das Objekt entfernt.

9 Konfiguration der On-Demand-Überprüfung

Erscheint in diesem Abschnitt das Wort PATH in einem Befehl, so bezieht es sich auf den zu überprüfenden Pfad.

9.1 Überprüfung aller Dateitypen

Standardmäßig überprüft Sophos Anti-Virus nur ausführbare Dateien. Um alle Dateien unabhängig von ihrem Typ zu überprüfen, geben Sie Folgendes ein:

```
savscan PATH -all
```

Dies dauert länger, als nur ausführbare Dateien zu überprüfen und kann die Leistung auf Servern gefährden. Es kann auch zu fehlerhaften Viren-/Spyware-Reports führen.

9.2 Überprüfung von Archiven

Sophos Anti-Virus kann Archive überprüfen, wenn es über die Option -archive verfügt.

```
savscan PATH -archive
```

Zu den Archivtypen, die überprüft werden können, gehören: ARJ, bzip2, CMZ, GZip, RAR, RPM, BZTAR, Zip.

Archive, die in andere Archive 'verschachtelt' sind (z.B. ein TAR-Archiv innerhalb eines Zip-Archivs), werden rekursiv überprüft.

Sie können aber auch die Überprüfung bestimmter Archivtypen angeben. Um beispielsweise eine Überprüfung in den TAR-Archiven durchzuführen, geben Sie Folgendes ein:

```
savscan PATH -tar
```

Oder um TAR- und Zip-Archive zu überprüfen, geben Sie Folgendes ein:

```
savscan PATH -tar -zip
```

Wenn Sie über zahlreiche komplexe Archive verfügen, so kann die Überprüfung entsprechend länger dauern. Denken Sie daran, wenn Sie einen Zeitplan für unbeaufsichtigte Überprüfungen erstellen.

Eine vollständige Liste der überprüften Archivtypen erhalten Sie mit der Option -vv.

9.3 Überprüfung remoter Computer

Standardmäßig überprüft Sophos Anti-Virus Objekte auf remoten Computern nicht (d.h., Sophos Anti-Virus übergeht keine remoten Mount Points). Um die Überprüfung remoter Computer zu aktivieren, geben Sie Folgendes ein:

```
savscan PATH --no-stay-on-machine
```

9.4 Deaktivieren der Überprüfung über Symbolic Links verknüpfter Objekte

Standardmäßig überprüft Sophos Anti-Virus symbolisch verknüpfte Objekte. Um diese Art der Überprüfung zu deaktivieren, geben Sie Folgendes ein:

```
savscan PATH --no-follow-symlinks
```

Um die mehrfache Überprüfung von Objekten zu vermeiden, verwenden Sie die Option --backtrack-protection.

9.5 Überprüfung nur des startenden Dateisystems

Sophos Anti-Virus kann so konfiguriert werden, dass keine Objekte nach dem startenden Dateisystem überprüft werden (d.h., es werden keine Mount Points übergangen). Geben Sie Folgendes ein:

```
savscan PATH --stay-on-filesystem
```

9.6 Befehlszeilenoptionen

Mit den in diesem Abschnitt aufgelisteten Befehlszeilenoptionen können Sie die Überprüfung und die Desinfektion konfigurieren. Es gibt:

- Optionen, die Sophos Anti-Virus für Linux mit Sophos Anti-Virus für UNIX und andere Plattformen gemeinsam hat (Abschnitt 9.6.1)
- Optionen, die Sophos Anti-Virus für Linux nur mit Sophos Anti-Virus für UNIX gemeinsam hat (Abschnitt 9.6.2)
- Optionen speziell für Sophos Anti-Virus für Linux (Abschnitt 9.6.3)

9.6.1 Befehlszeilenoptionen für Sophos Anti-Virus

Um die Bedeutung der Befehlszeilenoption umzukehren, setzen Sie ein 'n' vor den Befehl. Beispielsweise bezeichnet -nsc den Umkehrbefehl von -sc.

Um die Liste dieser Optionen am Bildschirm anzuzeigen, geben Sie Folgendes ein:

```
savscan -h
```

-all alle Dateien überprüfen

Wenn diese Option verwendet wird, überprüft Sophos Anti-Virus alle Dateien auf dem Dateisystem, anstatt nur die ausführbaren Dateien.

! Dies dauert länger, als nur ausführbare Dateien zu überprüfen und kann die Leistung auf Servern gefährden. Es kann auch zu fehlerhaften Viren-/Spyware-Reports führen.

-archive Archive überprüfen

Wird diese Option verwendet, so überprüft Sophos Anti-Virus Archive. Zu den Archivtypen, die überprüft werden, gehören ARJ, bzip2, CMZ, GZip, RAR, RPM, TAR, Zip.

Archive, die in andere Archive 'verschachtelt' sind (z.B. ein TAR-Archiv innerhalb eines Zip-Archivs), werden rekursiv überprüft.

Sie können aber auch die Überprüfung bestimmter Archivtypen angeben. Um beispielsweise eine Überprüfung in den TAR-Archiven durchzuführen, geben Sie Folgendes ein:

```
savscan PATH -tar
```

Oder um TAR- und Zip-Archive zu überprüfen, geben Sie Folgendes ein:

```
savscan PATH -tar -zip
```

Wenn Sie über zahlreiche komplexe Archive verfügen, so kann die Überprüfung entsprechend länger dauern. Denken Sie daran, wenn Sie einen Zeitplan für unbeaufsichtigte Überprüfungen erstellen.

Eine vollständige Liste der überprüften Archivtypen erhalten Sie mit der Option -vv.

-b Akustisches Signal bei Viren-/Spyware-Fund

Bei dieser Option gibt Sophos Anti-Virus ein akustisches Signal, wenn Viren/Spyware oder Fragmente von Viren/Spyware gefunden werden. Sie ist standardmäßig aktiviert.

-c Vor Desinfektion oder Löschen nach Bestätigung fragen

Bei dieser Option fragt Sophos Anti-Virus nach Ihrer Bestätigung, bevor Dateien desinfiziert oder gelöscht werden. Sie ist standardmäßig aktiviert.

-di Desinfizieren

Mit dieser Option führt Sophos Anti-Virus die automatische Desinfektion von Dateien, Programmen und Bootsektoren durch. Gehen Sie weiter zu Abschnitt 5.2.

-dn Namen von Dateien anzeigen, die überprüft werden

Diese Option zeigt die Dateien an, die gerade überprüft werden. Es werden Zeit und der Name des überprüften Objekts angezeigt.

-eec Erweiterte Fehlercodes verwenden

Bei dieser Option wird Sophos Anti-Virus angewiesen, erweiterte Fehlercodes zu verwenden. Einzelheiten sind in Abschnitt 3.6.1 zu finden.

-exclude Dateien von der Überprüfung ausschließen

Mit dieser Option können Sie festlegen, dass Objekte (Dateien, Verzeichnisse oder Dateisysteme) nach der Option in der Befehlszeile von der Überprüfung ausgeschlossen werden müssen.

Nach der Option -exclude können Sie mit der Option -include festlegen, dass Objekte nach der Option in der Befehlszeile überprüft werden müssen.

Zum Beispiel:

```
savscan fred harry -exclude tom peter -include bill
```

überprüft die Objekte fred, harry und bill, aber nicht tom oder peter.

Die Option -exclude kann für Dateien oder Verzeichnisse unter einem anderen Verzeichnis verwendet werden. Zum Beispiel:

```
savscan /home/fred -exclude /home/fred/games
```

überprüft alle Verzeichnisse von fred, schließt aber das Verzeichnis 'games' (und alle Verzeichnisse und Dateien darunter) aus.

-ext= Dateitypen, die als ausführbar definiert sind

Als Standardvorgabe überprüft Sophos Anti-Virus ausführbare DOS- und Windows-Dateien mit bestimmten Dateierweiterungen (starten Sie savscan mit der Option -w für eine Liste der verwendeten Dateierweiterungen).

Um zusätzliche Dateierweiterungen anzugeben, die Sophos Anti-Virus überprüfen soll, verwenden Sie die Option -ext= mit einer durch Komma getrennten Liste der Erweiterungen.

Um Dateierweiterungen von der Überprüfung auszuschließen, verwenden Sie -next.

Wenn Sie Dateien überprüfen möchten, die UNIX als ausführbar definiert, lesen Sie den Absatz über die examine-x-bit-Option in Abschnitt 9.6.2.

-f Ausführliche Überprüfung

Standardmäßig überprüft Sophos Anti-Virus nur die Teile einer Datei, bei denen es wahrscheinlich ist, dass sie Viren/Spyware enthalten. Bei einer 'ausführlichen' Überprüfung werden die gesamten Inhalte einer Datei geprüft. Sie kann durch diese Option festgelegt werden.

Eine ausführliche Überprüfung ist langsamer als eine Standardüberprüfung.

-h Hilfe

Diese Option listet alle Befehlszeilenoptionen auf, einschließlich LINUX-spezifischer Optionen.

-idedir= Alternatives Verzeichnis für Viren-/Spywarekennungsdateien (IDEs)

Mit dieser Option können Sie ein alternatives Verzeichnis für IDEs angeben. Zum Beispiel:

```
savscan PATH -idedir=/ide
```

weist Sophos Anti-Virus an, IDEs aus dem `/ide`-Verzeichnis, anstatt aus dem Standardverzeichnis zu lesen (normalerweise `/opt/sophos-av/lib/sav`).

-mime MIME-Dateien überprüfen

Mithilfe dieser Option kann Sophos Anti-Virus bei der Überprüfung auch MIME-Dateien prüfen. Standardmäßig überprüft Sophos Anti-Virus MIME-Dateien ***nicht***.

-oe Outlook Express Mailboxen überprüfen

Durch diese Option wird Sophos Anti-Virus angewiesen, im Rahmen einer Überprüfung auch Outlook Express-Mailboxen zu prüfen. Standardmäßig überprüft Sophos Anti-Virus Outlook Express-Mailboxen ***nicht***. Die Option -mime ist ebenfalls mit diesem Parameter zu verwenden.

-p=<Datei|Gerät> Bildschirmanzeige in Datei oder Gerät kopieren

Mit dieser Option sendet Sophos Anti-Virus alle Angaben an den Bildschirm und auch an eine bestimmte Datei oder ein bestimmtes Gerät. Zum Beispiel:

```
savscan PATH -p=log.txt
```

Dadurch sendet Sophos Anti-Virus die Bildschirmausgaben an die Datei log.txt.

-rec Rekursive Überprüfung durchführen

Diese Option weist Sophos Anti-Virus an, Verzeichnisse unter denen, die in der Befehlszeile angegeben werden, zu überprüfen. Sie ist standardmäßig aktiviert.

-remove Infizierte Objekte entfernen

Mit dieser Option entfernt Sophos Anti-Virus infizierte Objekte.

-s Stiller Start ohne Anzeige der überprüften Bereiche

Wird diese Option verwendet, so zeigt Sophos Anti-Virus die Dateien, die gerade überprüft werden, nicht auf dem Bildschirm an. Sie ist standardmäßig aktiviert.

-sc Komprimierte Dateien überprüfen

Wird diese Option verwendet, sucht Sophos Anti-Virus in Dateien nach Viren/Spyware, die mit PKLite, LZEXE und Diet komprimiert wurden. Sie ist standardmäßig aktiviert.

--stop-scan Überprüfung von 'Zip-Bomben' stoppen

Mit dieser Option stoppt Sophos Anti-Virus die Überprüfung von 'Zip-Bomben', wenn sie erkannt werden.

? 'Zip-Bomben' sind schädliche Dateien, die das Vorgehen von Antiviren-Scannern unterbrechen sollen. Diese Dateien verbergen sich normalerweise hinter unschuldig aussehenden Archivdateien, die, sobald sie für die Überprüfung entpackt werden, sehr viel Zeit, Festplattenspeicher oder Speicherplatz benötigen.

Zum Beispiel:

```
savscan -all /home/fred/misc --stop-scan
```

weist Sophos Anti-Virus an, alle Objekte (Dateien und Verzeichnisse) unter /home/fred/misc zu überprüfen und die Überprüfung zu unterbrechen, sobald 'Zip-Bomben' gefunden werden. Sobald eine 'Zip-Bombe' entdeckt wird, erscheint eine Meldung, die der Folgenden ähnelt:

```
Aborted checking /home/fred/misc/b.zip - appears to be
a 'zip bomb'
```

-v Versionsnummer

Wenn diese Option verwendet wird, zeigt Sophos Anti-Virus die Versionsnummer und eine Liste der Viren-/Spywarekennungen (IDEs) an, die gerade verwendet werden.

-vv Ausführliche Versionsinformation

Mit dieser Option zeigt Sophos Anti-Virus die Versionsnummer an und listet die gerade verwendeten Viren-/Spywarekennungen (IDEs), die überprüften Dateierweiterungen und die überprüften Archivtypen auf.

9.6.2 UNIX-spezifische Befehlszeilenoptionen

Die folgenden Optionen sind UNIX-spezifisch und können mit dem Präfix 'no-' in ihrer Bedeutung umgekehrt werden.

So kehrt zum Beispiel '--no-follow-symlinks' die Bedeutung von '--follow-symlinks' um.

--args-file=[Dateiname] Befehlszeilenargumente aus Datei lesen

Sophos Anti-Virus liest Befehlszeilenargumente aus Dateien. Zu den Argumenten können (Auflistungen von) Verzeichnisnamen, Dateinamen und Optionen gehören. Zum Beispiel:

```
savscan --args-file=scanlist
```

weist Sophos Anti-Virus an, Befehlszeilenargumente von der `scanlist`-Datei zu lesen. Sobald Sophos Anti-Virus das Ende der Datei erreicht hat, liest es die Argumente der Befehlszeile.

Lautet der [Dateiname] '-', so liest Sophos Anti-Virus Argumente aus stdin. Einige Befehlszeilenoptionen dürfen in der Datei nicht verwendet werden: -eec, -neec, -p=, -s, -ns, -dn und -ndn.

--backtrack-protection Rückverfolgung verhindern

Sophos Anti-Virus vermeidet es, dieselben Dateien mehr als einmal zu lesen ('Rückverfolgung'); dieses Problem kann sich aus symbolischen Links ergeben. Diese Option ist standardmäßig aktiviert.

--examine-x-bit Alle Objekte überprüfen, die UNIX als ausführbar definiert

Mit dieser Option überprüft Sophos Anti-Virus alle Objekte, die UNIX als ausführbar definiert, sowie alle Objekte mit Dateierweiterungen aus der Sophos Anti-Virus eigenen Liste der ausführbaren Dateien (für nähere Informationen starten Sie savscan mit der Option -vv). Diese Option ist standardmäßig deaktiviert.

--follow-symlinks Objekt überprüfen, auf das von symbolischen Links aus verwiesen wird

Sophos Anti-Virus überprüft Objekte, auf die mit symbolischen Links verwiesen wird. Diese Option ist standardmäßig aktiviert.

--preserve-backtrack Rückverfolgungsdaten aufbewahren

Sophos Anti-Virus speichert die Rückverfolgungsdaten für die Dauer der Überprüfung. Diese Option ist standardmäßig aktiviert.

--quarantine Infizierte Dateien in Quarantäne verschieben

Wird diese Option verwendet, verschiebt Sophos Anti-Virus infizierte Dateien in Quarantäne. Dies geschieht, indem Besitzer und Rechte für diese Datei geändert werden.

Wenn Sie die Desinfektion spezifiziert haben, versucht Sophos Anti-Virus, die Datei zu desinfizieren und stellt die Datei nur dann unter Quarantäne, wenn die Desinfektion fehlschlägt.

Wenn Sie nichts anderes angegeben haben, ändert Sophos Anti-Virus den Besitzer der Datei um in den Benutzer, der Sophos Anti-Virus gestartet hat, und ändert die Dateirechte um in -r -------- (0400).

Die Option können Sie auch mit anderen Parametern verwenden:

```
uid=NNN
user=USERNAME
gid=NNN
group=GROUP-NAME
mode=PPP
```

Sie können nicht mehr als einen Parameter jedes Typs angeben (d.h., Sie können keinen Benutzernamen zweimal oder eine uid und einen Benutzernamen eingeben).

Für jeden Parameter, den Sie nicht setzen, werden die Standardeinstellungen angewendet (wie unten angegeben).

Zum Beispiel:

```
savscan fred -quarantine:user=virus,group=virus,mode=0400
```

Hier wird der Besitzer der infizierten Datei zu virus, der Gruppenbesitzer zu virus und die Dateirechte werden zu -r-------- geändert. Das bedeutet, dass sich die Datei im Besitz des Benutzers virus und Gruppenvirus befindet, aber *nur* der Benutzer virus kann auf die Datei zugreifen (er hat nur Leserechte). Die Datei kann von keinem anderen Benutzer bearbeitet werden (ausgenommen von root).

Möglicherweise müssen Sie als spezieller Benutzer oder als Superuser angemeldet sein, um den Besitzer und die Rechte ändern zu können.

--reset-atime Zugriffszeit für Dateien neu einstellen

Nachdem Sophos Anti-Virus eine Datei überprüft hat, verändert es die Zugriffszeit wieder auf den Zeitpunkt, der vor der Überprüfung angegeben wurde. Wenn eine Datei jedoch desinfiziert wird, werden Zugriffs- und Veränderungszeiten aktualisiert. Diese Option ist standardmäßig aktiviert.

Es kann sein, dass Ihr Archiver stets ein Backup für alle Dateien erstellt, die überprüft worden sind. Der Grund dafür kann darin liegen, dass die Neueinstellung der Zeitmarke atime dazu führt, dass die Zeitmarke Inode Status-Changed Time (ctime) geändert wird. In diesem Fall führen Sie den Befehl savscan mit der Option --no-reset-atime aus.

--show-file-details Besitzerdetails der Datei anzeigen

Mit dieser Option zeigt Sophos Anti-Virus Details über den Besitzer und Rechte der Datei an, wenn Dateinamen angezeigt oder in ein Protokoll geschrieben werden.

--skip-special 'Special'-Objekte nicht überprüfen

Sophos Anti-Virus überprüft spezielle Objekte, wie /dev, /proc, /Geräte usw. nicht. Diese Option ist standardmäßig aktiviert.

--stay-on-filesystem Verlassen Sie nicht das startende Dateisystem

Mit dieser Option überprüft Sophos Anti-Virus nur das startende Dateisystem, d.h. es geht nicht über Mount-Points.

--stay-on-machine Verlassen Sie nicht den startenden Computer

Sophos Anti-Virus überprüft nur den startenden Computer, es geht nicht über remote Mount Points. Diese Option ist standardmäßig aktiviert.

9.6.3 Linux-spezifische Befehlszeilenoptionen

Die folgenden Überprüfungsoptionen für den Bootsektor sind nur bei Sophos Anti-Virus für Linux verfügbar.

-bs=xxx, xxx,... Bootsektor von spezifischen logischen Laufwerken überprüfen

Sophos Anti-Virus überprüft die Bootsektoren der spezifischen logischen Laufwerke, wobei xxx den Namen des Laufwerks bezeichnet (beispielsweise /dev/fd0 oder /dev/hda1). Das Diskettenlaufwerk wird bei dieser Option als logisches Gerät angesehen.

Mit dieser Option können Sie auch die Bootsektoren von Disketten überprüfen, die für andere Betriebssysteme (z.B. Windows und DOS) erstellt wurden.

--bs Alle bekannten Bootsektoren überprüfen

Sophos Anti-Virus entnimmt Informationen aus der Partitionstabelle aller physischen Laufwerke, die ihm bekannt sind und überprüft sodann alle Bootsektoren der logischen Laufwerke. Dazu gehören auch nicht-Linux-Bootsektoren (z.B. Windows und DOS).

-cdr= Scan CD Boot-Image

Um das Boot-Image einer bootfähigen CD zu überprüfen, verwenden Sie die Option -cdr. Zum Beispiel:

```
savscan -cdr=/dev/cdrom
```

überprüft das Boot-Image (sofern es vorhanden ist) der CD auf dem Gerät /dev/cdrom. Wenn Sophos Anti-Virus ein Boot-Image findet, überprüft es den Bootsektor des Image auf Bootsektor-Viren.

Um in allen Dateien des Boot-Image nach Programmviren zu suchen, deren Dateityp in der Liste der ausführbaren Dateien von Sophos Anti-Virus aufgeführt ist, verwenden Sie die Option -loopback. Zum Beispiel:

```
savscan -cdr=/dev/cdrom -loopback
```

überprüft das Boot-Image (sofern es vorhanden ist) der CD auf dem Gerät /dev/cdrom. Wenn Sophos Anti-Virus ein Boot-Image findet, so überprüft es den Bootsektor dieses Image auf Bootsektor-Viren und überprüft alle Dateien dieses Image auf Viren, deren Dateityp in der Liste der ausführbaren Dateien enthalten ist.

--mbr Master Bootsektoren überprüfen

Sophos Anti-Virus versucht, Masterbootsektoren für alle physischen Laufwerke auf dem System zu überprüfen.

10 Konfiguration von Alarmen

Wenn Sie einen einzelnen Computer konfigurieren, der sich in einem Netzwerk befindet, so kann solch eine Konfiguration verloren gehen, wenn der Computer eine neue Konsolen-basierte Konfiguration herunterlädt.

Sie können Sophos Anti-Virus so konfigurieren, dass es einen Alarm sendet, wenn es Viren/Spyware, Überprüfungs- oder einen anderen Fehler findet. Alarme können in verschiedenen Sprachen und auf folgende Arten versendet werden:

- Desktop Pop-Ups (nur bei der On-Access-Überprüfung)
- Befehlszeile (nur On-Access-Überprüfung)
- E-Mail (On-Access- und On-Demand-Überprüfung)

10.1 Konfiguration von Desktop Pop-Up-Alarmen

Standardmäßig sind Pop-Up-Alarme aktiviert. Sie werden in der Sprache des Computers gesendet, der den Alarm ausgibt.

Die zusätzlichen Meldungen, die unten beschrieben werden, werden nicht übersetzt.

Befehlszeile

Um Desktop Pop-Up-Alarme zu aktivieren, müssen Sie die Parameter UINotifier und UIpopupNotification auf 'enabled' stellen. UINotifier bietet die gesamte Kontrolle von Desktop-Popup- und Befehlszeilenalarmen. UIpopupNotification kontrolliert nur die Desktop-Popup-Alarme. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig UINotifier enabled
```

```
/opt/sophos-av/bin/savconfig UIpopupNotification enabled
```

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird. Die Standardmeldung ist englisch. Um sie zu ändern, verwenden Sie den Parameter 'UIContactMessage'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig UIContactMessage 'Contact IT'
```

Dieselben Benachrichtigungstexte werden für Desktop Pop-Up- und Befehlszeilenalarme verwendet.

Um Desktop Pop-Up-Alarme zu deaktivieren, geben Sie Folgendes ein:

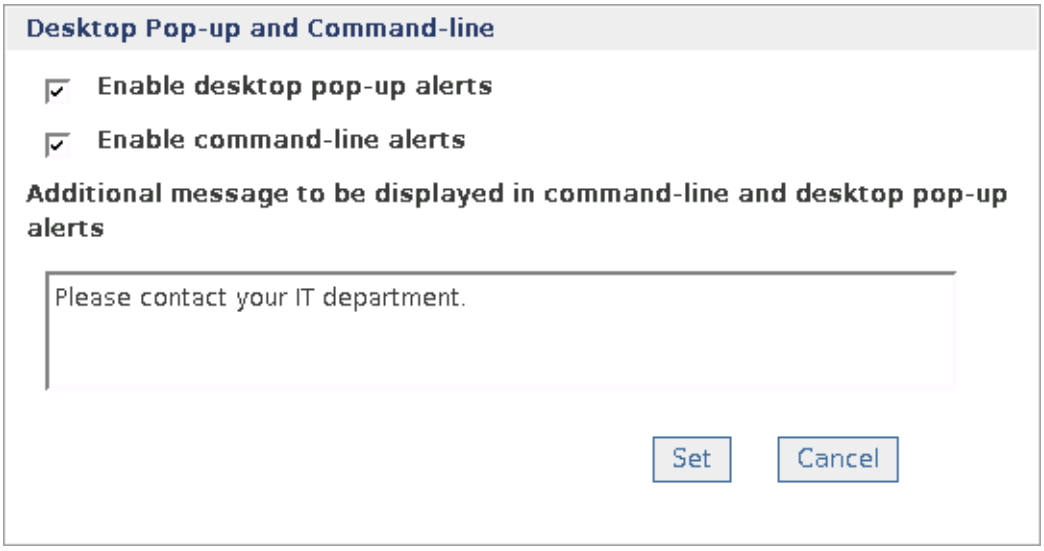
```
/opt/sophos-av/bin/savconfig UIpopupNotification disabled
```

Um sowohl Desktop Pop-Up- als auch Befehlszeilenalarme zu deaktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

GUI

Um Desktop Pop-Up-Alarme zu konfigurieren, gehen Sie auf die Seite **Alerts Configuration** in das Fenster **Desktop Pop-up and Command-line**.


Desktop Pop-up and Command-line
Enable desktop pop-up alerts
Enable command-line alerts
Additional message to be displayed in command-line and desktop pop-up alerts
Please contact your IT department.
Set
Cancel

Konfigurieren Sie Desktop Pop-Up-Alarme wie nachfolgend beschrieben. Wenn Sie dies getan haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

Um Desktop Pop-Up-Alarme zu aktivieren, klicken Sie das Kontrollkästchen **Enable desktop pop-up alerts** an.

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird. Die Standardmeldung ist englisch. Um sie zu ändern, geben Sie etwas in das Textfeld ein.

Dieselben Benachrichtigungstexte werden für Desktop Pop-Up- und Befehlszeilenalarme verwendet.

Um Desktop Pop-Up-Alarme zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Enable desktop pop-up alerts**.

10.2 Konfiguration von Befehlszeilenalarmen

Standardmäßig sind Befehlszeilenalarme aktiviert. Sie werden in der Sprache des Computers gesendet, der den Alarm ausgibt.

Die zusätzlichen Meldungen, die unten beschrieben werden, werden nicht übersetzt.

Befehlszeile

Um Befehlszeilenalarme zu aktivieren, müssen Sie die Parameter UINotifier und UIpopupNotification auf 'enabled' stellen. UINotifier bietet die gesamte Kontrolle von Desktop-Popup- und Befehlszeilenalarmen. UIttyNotification kontrolliert nur Befehlszeilenalarme. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig UINotifier enabled
```

```
/opt/sophos-av/bin/savconfig UIttyNotification enabled
```

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird. Die Standardmeldung ist englisch. Um sie zu ändern, verwenden Sie den Parameter 'UIContactMessage'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig UIContactMessage 'Contact IT'
```

Dieselben Benachrichtigungstexte werden für Desktop Pop-Up- und Befehlszeilenalarme verwendet.

Um Befehlszeilenalarme zu deaktivieren, geben Sie ein:

```
/opt/sophos-av/bin/savconfig UIttyNotification disabled
```

Um sowohl Desktop Pop-Up- als auch Befehlszeilenalarme zu deaktivieren, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

GUI

Um Befehlszeilenalarme zu konfigurieren, gehen Sie auf die Seite **Alerts Configuration** in das Fenster **Desktop Pop-up and Command-line**.

Desktop Pop-up and Command-line
Enable desktop pop-up alerts
Enable command-line alerts
Additional message to be displayed in command-line and desktop pop-up alerts
Please contact your IT department.
Set
Cancel

Konfigurieren Sie Befehlszeilenalarme wie untenstehend beschrieben. Wenn Sie dies getan haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

Um Befehlszeilenalarme zu aktivieren, klicken Sie das Kontrollkästchen **Enable command-line alerts** an.

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird. Die Standardmeldung ist englisch. Um sie zu ändern, geben Sie etwas in das Textfeld ein.

Dieselben Benachrichtigungstexte werden für Desktop Pop-Up- und Befehlszeilenalarme verwendet.

Um Befehlszeilenalarme zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Enable command-line alerts**.

10.3 Konfiguration von E-Mail-Benachrichtigungen

Der Standard für E-Mail-Alarme lautet folgendermaßen:

- aktiviert
- gesendet, wenn Viren/Spyware erkannt werden, es einen Überprüfungsfehler gibt oder ein Ereignis im Sophos Anti-Virus Protokoll erfasst wird
- ein Alarm wird nur gesendet, wenn ein schwerwiegendes (fatal) Ereignis vorliegt
- er wird gesendet an: root@localhost

Hostname und Port des SMTP-Servers lauten localhost:25.

10.3.1 Allgemeine Einstellungen

Befehlszeile

Um E-Mail-Benachrichtigungen zu aktivieren, setzen Sie den Parameter 'EmailNotifier' auf 'enabled':

```
/opt/sophos-av/bin/savconfig EmailNotifier enabled
```

Um den HOST-Namen oder die IP-Adresse des SMTP-Servers festzulegen, verwenden Sie den Parameter EmailServer. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig EmailServer 171.17.31.184
```

Um die Sprache für die E-Mail-Benachrichtigungen festzulegen, verwenden Sie den Parameter 'EmailLanguage'. Zurzeit sind nur ‘en’, ‘English’ und 'Japanese' gültige Einträge. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig EmailLanguage Japanese
```

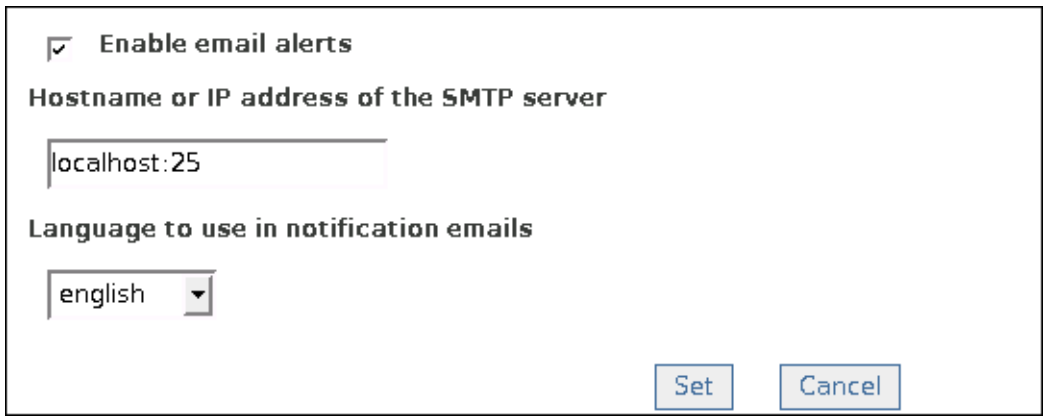
Diese Sprachauswahl trifft nur für den Alarm selbst zu, jedoch nicht für die zusätzlichen Meldungen, die unten beschrieben werden.

Um keine E-Mail-Benachrichtigungen zu senden, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig EmailNotifier disabled
```

GUI

Um E-Mail-Benachrichtungen über die GUI zu konfigurieren, gehen Sie zu der Seite **Alerts Configuration** in das Fenster **Email**.



Um das Versenden von E-Mail-Benachrichtigungen zu aktivieren, klicken Sie das Kontrollkästchen **Enable email alerts** an.

Um den HOST-Namen oder die IP-Adresse des SMTP-Servers festzulegen, geben Sie die Adresse in das Textfenster **Hostname or IP address of the SMTP server** ein.

Um die Sprache für die E-Mail-Benachrichtigungen festzulegen, wählen Sie die Sprache in dem Drop-Down-Listenfeld namens **Language to use in notification emails**.

Diese Sprachauswahl trifft nur für den Alarm selbst zu, jedoch nicht für die zusätzlichen Meldungen, die unten beschrieben werden.

Um keine E-Mail-Benachrichtigungen zu versenden, deaktivieren Sie das Kontrollkästchen **Enable email alerts**.

Wenn Sie die Konfiguration der E-Mail-Benachrichtigungen abgeschlossen haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

10.3.2 E-Mail-Empfänger

Befehlszeile

Um festzulegen, wer E-Mail-Benachrichtigungen empfängt, verwenden Sie den Parameter 'Email'. Sie können mehr als einen Empfänger festlegen. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig Email admin@localhost
```

GUI

Um festzulegen, wer E-Mail-Benachrichtigungen erhält, fügen Sie Empfänger zu der Liste von **Email recipients** hinzu oder entfernen Sie sie.

Um neue E-Mail-Empfänger zu der Liste hinzuzufügen, geben Sie den Text in das Adressenfeld ein und klicken Sie auf **Add New Entry**.

Um einen E-Mail-Empfänger von der Liste zu löschen, wählen Sie ihn aus und klicken Sie auf **Remove Selected Entry**.

10.3.3 Was passiert, wenn Viren/Spyware erkannt werden

Befehlszeile

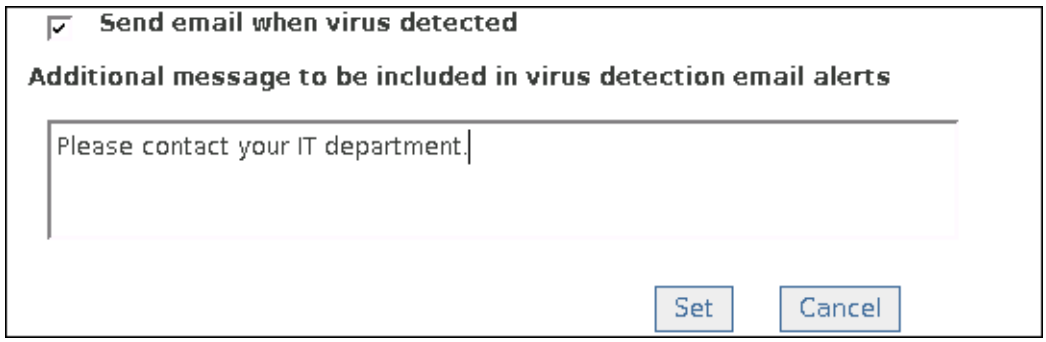
Um die Funktion zu aktivieren, dass bei Auffinden von Viren/Spyware eine E-Mail-Benachrichtigung gesendet wird, setzen Sie den Parameter 'SendThreatEmail' auf 'enabled':

```
/opt/sophos-av/bin/savconfig SendThreatEmail enabled
```

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird, wenn Viren/Spyware erkannt werden. Die Standardmeldung ist englisch. Um sie zu ändern, verwenden Sie den Parameter 'ThreatMessage'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig ThreatMessage 'Contact IT'
```

GUI


Send email when virus detected
Additional message to be included in virus detection email alerts
Please contact your IT department.
Set
Cancel

Um E-Mail-Benachrichtungen beim Auffinden von Viren/Spyware zu senden, klicken Sie das Kontrollkästchen **Send email when virus detected** an.

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird, wenn Viren/Spyware erkannt werden. Die Standardmeldung ist englisch. Um sie zu ändern, geben Sie etwas in das Textfeld ein.

Wenn Sie die Konfiguration der E-Mail-Benachrichtigungen abgeschlossen haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

10.3.4 Was passiert bei einem Überprüfungsfehler

Befehlszeile

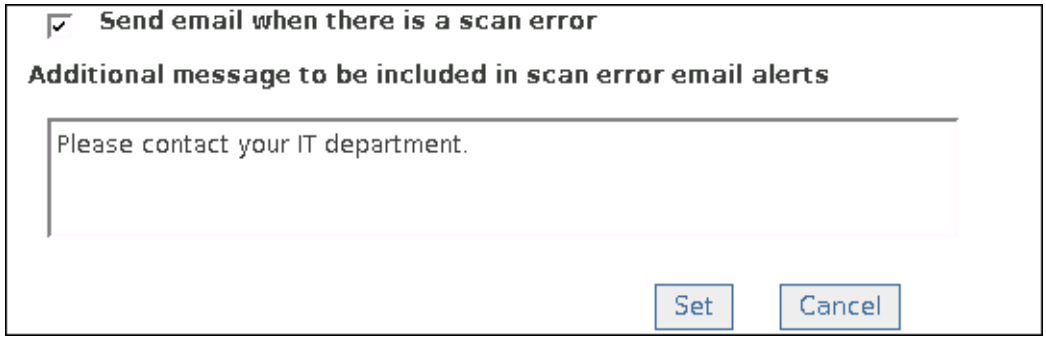
Um die Funktion zu aktivieren, dass bei einem Überprüfungsfehler eine E-Mail-Benachrichtigung gesendet wird, setzten Sie den Parameter SendErrorEmail auf 'enabled':

```
/opt/sophos-av/bin/savconfig SendErrorEmail enabled
```

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird, wenn ein Überprüfungsfehler auftritt. Die Standardmeldung ist englisch. Um sie zu ändern, verwenden Sie den Parameter 'ScanErrorMessage'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig ScanErrorMessage 'Contact IT'
```

GUI


Send email when there is a scan error
Additional message to be included in scan error email alerts
Please contact your IT department.
Set
Cancel

Um E-Mail-Benachrichtigungen beim Auftreten eines Überprüfungsfehlers zu versenden, klicken Sie das Kontrollkästchen **Send email when there is a scan error** an.

Sie können zusätzlich zum Alarm festlegen, welche Meldung gesendet wird, wenn ein Überprüfungsfehler auftritt. Die Standardmeldung ist englisch. Um sie zu ändern, geben Sie etwas in das Textfeld ein.

Wenn Sie die Konfiguration der E-Mail-Benachrichtigungen abgeschlossen haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

10.3.5 Was passiert, wenn ein Ereignis protokolliert wird

Befehlszeile

Sie können zusätzlich zu dem Alarm festlegen, welche Meldung gesendet wird, wenn ein Ereignis im Sophos Anti-Virus Protokoll erfasst wird. Die Standardmeldung ist englisch. Um sie zu ändern, verwenden Sie den Parameter 'LogMessage'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig LogMessage 'Contact IT'
```

GUI

Sie können festlegen, welche Meldung gesendet wird, wenn ein Ereignis im Sophos Anti-Virus Protokoll erfasst wird. Die Standardmeldung ist englisch. Um sie zu ändern, geben Sie etwas in das Textfeld ein.

Wenn Sie die Konfiguration der E-Mail-Benachrichtigungen abgeschlossen haben, klicken Sie auf **Set**, um die Änderungen anzunehmen. Um Änderungen rückgängig zu machen, die Sie vorgenommen haben, seit Sie das letzte Mal auf **Set** geklickt haben, klicken Sie auf **Cancel**.

11 Konfiguration des Sophos Anti-Virus-Protokolls

Wenn Sie einen einzelnen Computer konfigurieren, der sich in einem Netzwerk befindet, so kann solch eine Konfiguration verloren gehen, wenn der Computer eine neue Konsolen-basierte Konfiguration herunterlädt.

Standardmäßig werden die Überprüfungen in dem Sophos Anti-Virus-Protokoll aufgeführt. Wenn das Protokoll 1 MB erreicht, wird davon automatisch ein Backup erstellt und ein neues Protokoll begonnen. Um die Standardanzahl von Protokollen anzusehen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB
```

Um die maximale Anzahl von Protokollen festzulegen, verwenden Sie den Parameter 'LogMaxSizeMB'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig LogMaxSizeMB 50
```

Der Pfad des Protokolls lautet /opt/sophos-av/log/savd.log.

12 Konfiguration der Sophos Anti-Virus GUI

Wenn Sie einen einzelnen Computer konfigurieren, der sich in einem Netzwerk befindet, so kann solch eine Konfiguration verloren gehen, wenn der Computer eine neue Konsolen-basierte Konfiguration herunterlädt.

Sie können die Sophos Anti-Virus GUI auf zwei Arten konfigurieren:

- Über das Dienstprogramm savsetup oder
- Über den Befehl savconfig.

savsetup

1. Führen Sie auf dem Computer das Dienstprogramm savsetup aus, das sich in dem bin-Unterverzeichnis der Installation befindet:

   ```
   /opt/sophos-av/bin/savsetup
   ```

2. Sie müssen nun die Aktivität auswählen, die Sie durchführen möchten. Wählen Sie **Sophos Anti-Virus GUI configuration**.
3. Das Dienstprogramm stellt Ihnen mehrere Fragen zur GUI. Geben Sie Ihre Antworten ein, um die GUI zu konfigurieren.

savconfig

Um den HTTP-Port der GUI festzulegen, verwenden Sie den Parameter HttpPort. (Es kann nicht über einen *externen* Port auf die GUI zugegriffen werden.) Um den Standard-Port zu sehen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig -s query HttpPort
```

Um den Port zu ändern, geben Sie z.B. Folgendes ein:

```
/opt/sophos-av/bin/savconfig HttpPort 1880
```

Um den Benutzernamen zum Gebrauch der GUI einzustellen, verwenden Sie die Parameter 'HttpUsername'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig HttpUsername sysadmin
```

Um das Kennwort zum Gebrauch der GUI einzustellen, verwenden Sie den Parameter 'HttpPassword'. Geben Sie beispielsweise Folgendes ein:

```
/opt/sophos-av/bin/savconfig HttpPassword 0jf09jf
```

Diese Einstellungen werden erst übernommen, wenn der GUI-Dämon neu gestartet wird. Um dies manuell vorzunehmen, müssen Sie die GUI schließen und in der Befehlszeile Folgendes eingeben:

```
/etc/init.d/sav-web restart
```

Aktualisierung von Sophos Anti-Virus

Sofortige Aktualisierung von Sophos Anti-Virus

Kernel-Support

Konfiguration der Aktualisierung

13 Sofortige Aktualisierung von Sophos Anti-Virus

Wenn Sie die automatische Aktualisierung aktiviert haben, wird Sophos Anti-Virus automatisch aktualisiert.

Um einen Computer in dem Zeitraum zwischen automatischen Updates zu aktualisieren, führen Sie bitte das Aktualisierungs-Skript aus:

```
/opt/sophos-av/bin/savupdate
```

14 Kernel-Support

14.1 Support für neue Kernel-Versionen

Wenn einer der von Sophos Anti-Virus unterstützten Linux-Hersteller ein Update des Linux Kernel herausgibt, gibt Sophos ein Update des Sophos Kernel-Oberflächenmoduls heraus, um das Update zu unterstützen. Wenn Sie das Update eines Linux Kernels *vor* dem Update des entsprechenden Sophos Kernel-Oberflächenmoduls installieren, wird die On-Access-Überprüfung deaktiviert und ein Fehler gemeldet.

Um dieses Problem zu vermeiden, müssen Sie sicherstellen, dass das Update des entsprechenden Sophos Kernel-Oberflächenmoduls bereits vorhanden ist, bevor Sie das Update des Linux Kernels aktualisieren. Eine Liste unterstützter Linux-Versionen und -Updates finden Sie im Sophos Support Knowledgebase Artikel 14377 (www.sophos.de/support/knowledgebase/article/14377.html). Wenn das entsprechende Update des Sophos Kernel-Oberflächenmoduls aufgelistet ist, steht es zum Herunterladen zur Verfügung. Wenn Sie die automatische Aktualisierung aktiviert haben, wird Sophos Anti-Virus automatisch aktualisiert. Um einen Computer in dem Zeitraum zwischen automatischen Updates zu aktualisieren, führen Sie das Aktualisierungs-Skript aus:

```
/opt/sophos-av/bin/savupdate
```

Danach können Sie das Update des Linux Kernels anwenden.

14.2 Support für kundenspezifische Kernel

Dieses Handbuch beschreibt die Konfiguration von Updates zur Unterstützung kundenspezifischer Linux Kernel nicht. Siehe Sophos Support Knowledgebase Artikel 13503 (www.sophos.de/support/knowledgebase/article/13503.html).

15 Konfiguration der Updates

Wenn Sie Sophos Anti-Virus für Linux mit Enterprise Console verwalten, müssen Sie Updates über die Konsole konfigurieren. Informationen dazu finden Sie in der Konsolenhilfe und nicht in diesem Abschnitt.

15.1 Grundkonzepte

Update-Server

Ein *Update-Server* ist ein Computer, auf dem Sie Sophos Anti-Virus für Linux installiert haben und der auch als Update-Quelle für andere Computer dient. Diese anderen Computer sind entweder Update-Server oder Update-Endpoints, je nachdem wie Sie Sophos Anti-Virus im Netzwerk einsetzen.

Update-Endpoint

Ein *Update-Endpoint* ist ein Computer, auf dem Sie Sophos Anti-Virus für Linux installiert haben und der nicht als Update-Quelle für andere Computer dienen muss.

Primäre Update-Quelle

Die *primäre Update-Quelle* ist der Speicherort der Updates, auf den ein Computer gewöhnlich zugreift. Dazu sind eventuell Zugangsdaten erforderlich.

Sekundäre Update-Quelle

Die *sekundäre Update-Quelle* ist der Speicherort der Updates, auf den ein Computer zugreift, wenn er auf die primäre Update-Quelle nicht zugreifen kann. Dazu sind eventuell Zugangsdaten erforderlich.

15.2 Überprüfen der automatischen Update-Konfiguration eines Computers

1. Starten Sie auf dem Computer, den Sie überprüfen möchten, das Dienstprogramm 'savsetup':

   ```
   /opt/sophos-av/bin/savsetup
   ```

2. Sie müssen jetzt Ihr gewünschtes Vorgehen auswählen. Wählen Sie **Auto-updating configuration**.

3. Wählen Sie **Display update configuration**, um die derzeitige Konfiguration zu sehen.

15.3 Konfiguration des Update-Servers, um direkt von Sophos zu aktualisieren

1. Starten Sie auf dem Update-Server das Dienstprogramm 'savsetup':

   ```
   /opt/sophos-av/bin/savsetup
   ```

2. Sie müssen jetzt Ihr gewünschtes Vorgehen auswählen. Wählen Sie **Auto-updating configuration**.

3. Wählen Sie die Option zur Konfiguration von Sophos als primäre Update-Quelle. Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen und das Kennwort ein, die in Ihrer Lizenz enthalten sind.

4. Sie müssen angeben, ob Sie auf Sophos über einen Proxy zugreifen. Wenn ja, geben Sie 'Y' und dann die Proxy-Details ein.

15.4 Konfiguration mehrerer Update-Endpoints zum Update vom Update-Server

Um die Konfiguration eines einzelnen Update-Endpoints zu ändern, siehe Abschnitt 15.6.

Auf dem Update-Server aktualisieren Sie die nicht aktivierte Konfigurationsdatei im CID und wenden dann die Änderungen auf die aktive Konfigurationsdatei an, damit sie für die Update-Endpoints beim nächsten Update zum Download bereitstehen. Im nachfolgenden Vorgang stellt CONFIG-FILE den Pfad der nicht aktivierten Konfigurationsdatei dar.

1. Stellen Sie die primäre Update-Quelladresse auf den Speicherort des CID mithilfe des Parameters 'PrimaryUpdateSourcePath' ein. Sie können entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem wie Sie den Update-Server eingestellt haben. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
   ```

2. Sollte die primäre Update-Quelle eine Authentifizierung benötigen, stellen Sie den Benutzernamen und das Kennwort mithilfe des jeweiligen Parameters 'PrimaryUpdateUsername' und 'PrimaryUpdatePassword' ein. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdateUsername 'fred'

   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdatePassword 'j23rjjfwj'
   ```

3. Wenn Sie über einen Proxy auf die primäre Update-Quelle zugreifen, stellen Sie die Adresse, den Benutzernamen und das Kennwort des Proxy-Servers mithilfe der jeweiligen Parameter 'PrimaryUpdateProxyAddress', 'PrimaryUpdateProxyUsername' und 'PrimaryUpdateProxyPassword' ein. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'

   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdateProxyUsername 'penelope'

   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     PrimaryUpdateProxyPassword 'fj202jrjf'
   ```

4. Verwenden Sie das Dienstprogramm 'addcfg', um die Änderungen auf die aktive Konfigurationsdatei anzuwenden, damit sie für die Update-Endpoints beim nächsten Update zum Download bereitstehen.

   ```
   /opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
   ```

15.5 Konfiguration mehrerer Update-Endpoints zum direkten Update von Sophos, wenn der Update-Server nicht verfügbar ist

Um die Konfiguration eines einzelnen Update-Endpoints zu ändern, siehe Abschnitt 15.7.

Auf dem Update-Server aktualisieren Sie die nicht aktivierte Konfigurationsdatei im CID und wenden dann die Änderungen auf die aktive Konfigurationsdatei an, damit sie für die Update-Endpoints beim nächsten Update zum Download bereitstehen. Im nachfolgenden Vorgang stellt CONFIG-FILE den Pfad der nicht aktivierten Konfigurationsdatei dar.

1. Stellen Sie die sekundäre Update-Quelladresse auf 'sophos:' mithilfe des Parameters 'SecondaryUpdateSourcePath'. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdateSourcePath 'sophos:'
   ```

2. Stellen Sie den Benutzernamen für die sekundäre Update-Quelle mithilfe des Parameters 'SecondaryUpdateUsername' auf den in Ihrer Lizenz enthaltenen. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdateUsername 'cust123'
   ```

3. Stellen Sie das Kennwort für die sekundäre Update-Quelle mithilfe des Parameters 'SecondaryUpdatePassword' auf das in Ihrer Lizenz enthaltene. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdatePassword 'j23rjjfwj'
   ```

4. Wenn Sie über einen Proxy auf das Internet zugreifen, stellen Sie Adresse, Benutzernamen und Kennwort des Proxy-Servers mithilfe des jeweiligen Parameters 'SecondaryUpdateProxyAddress', 'SecondaryUpdateProxyUsername' und 'SecondaryUpdateProxyPassword' ein. Geben Sie beispielsweise Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'

   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdateProxyUsername 'fred'

   /opt/sophos-av/bin/savconfig -f CONFIG-FILE -c
     SecondaryUpdateProxyPassword 'fj202jrjf'
   ```

5. Verwenden Sie das Dienstprogramm 'addcfg', um die Änderungen auf die aktive Konfigurationsdatei anzuwenden, damit sie für die Update-Endpoints beim nächsten Update zum Download bereitstehen.

   ```
   /opt/sophos-av/update/cache/Primary/addcfg.sh -f CONFIG-FILE
   ```

15.6 Konfiguration eines einzelnen Update-Endpoints zum Update vom Update-Server

Um die Konfiguration für mehrere Update-Endpoints zu ändern, siehe Abschnitt 15.4.

Dieser Abschnitt geht davon aus, dass der Update-Server die *primäre* Update-Quelle für diesen Computer ist. Sollte er jedoch die *sekundäre* Update-Quelle sein, verwenden Sie die unten erwähnten sekundären Optionen und Parameter.

1. Starten Sie auf dem Computer, den Sie konfigurieren möchten, das Dienstprogramm 'savsetup':

   ```
   /opt/sophos-av/bin/savsetup
   ```

2. Sie müssen jetzt Ihr gewünschtes Vorgehen auswählen. Wählen Sie **Auto-updating configuration**.

3. Wählen Sie die Option zur Konfiguration Ihres Servers als primäre (oder sekundäre) Update-Quelle. Wenn Sie dazu aufgefordert werden, geben Sie die Adresse der Quelle und, falls erforderlich, den Benutzernamen und das Kennwort ein. Sie können entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem wie Sie den Update-Server eingestellt haben.

4. Sie müssen angeben, ob Sie auf Sophos über einen Proxy zugreifen. Wenn ja, geben Sie 'Y' und dann die Proxy-Details ein.

15.7 Konfiguration eines einzelnen Endpoints zum direkten Update von Sophos

Um die Konfiguration für mehrere Update-Endpoints zu ändern, siehe Abschnitt 15.5.

Dieser Abschnitt geht davon aus, dass Sophos die *primäre* Update-Quelle für diesen Computer ist. Sollte er jedoch die *sekundäre* Update-Quelle sein, verwenden Sie die unten erwähnten sekundären Optionen und Parameter.

1. Starten Sie auf dem Computer, den Sie konfigurieren möchten, das Dienstprogramm 'savsetup':

   ```
   /opt/sophos-av/bin/savsetup
   ```

2. Sie müssen jetzt Ihr gewünschtes Vorgehen auswählen. Wählen Sie **Auto-updating configuration**.

3. Wählen Sie die Option zur Konfiguration von Sophos als primäre (oder sekundäre) Update-Quelle. Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen und das Kennwort ein, die in Ihrer Lizenz enthalten sind.

4. Sie müssen angeben, ob Sie auf Sophos über einen Proxy zugreifen. Wenn ja, geben Sie 'Y' und dann die Proxy-Details ein.

Fehlersuche

16 Fehlersuche

In diesem Abschnitt sind Lösungen für einige gängige Probleme zu finden, die bei der Verwendung von Sophos Anti-Virus auftreten können. (Weitere Informationen über Sophos Anti-Virus Fehlercodes für On-Demand-Überprüfungen sind in Abschnitt 3.6 zu finden.)

16.1 Es ist nicht möglich, einen Befehl auszuführen

Wenn Sie einen Befehl nicht ausführen können, haben Sie wahrscheinlich nicht ausreichende Rechte. Versuchen Sie, sich mit Root-Rechten anzumelden.

16.2 Die Konfiguration für den Ausschluss wurde nicht umgesetzt

Wenn Sie Sophos Anti-Virus so konfigurieren, dass Objekte in die Überprüfung eingeschlossen werden, die vorher davon ausgeschlossen waren, bleiben sie mitunter auch weiterhin ausgeschlossen. Versuchen Sie, den Cache an Dateien zu leeren, die bereits überprüft worden sind:

```
echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
```

```
echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
```

16.3 Man-Seite wurde nicht gefunden

Wird diese Meldung angezeigt, wenn Sie versuchen, die Man-Seite von Sophos Anti-Virus zu betrachten, müssen Sie wahrscheinlich Ihre Systemeinstellungen ändern. Stellen Sie sicher, dass die Umgebungsvariable MANPATH in Ihrem Anmeldeskript oder Profil folgenden Pfad enthält: /usr/local/man. Ist dieser Pfad nicht darin enthalten, fügen Sie ihn zu der Umgebungsvariablen hinzu, wie in nachstehenden Beispielen verdeutlicht. Verändern Sie die bestehenden Einstellungen nicht.

Wenn Sie die Shell sh, ksh oder bash verwenden, geben Sie Folgendes ein:

```
MANPATH=$MANPATH:/usr/local/man
export MANPATH
```

Wenn Sie die csh oder tsh shell starten, geben Sie Folgendes ein:

```
setenv MANPATH [Einträge]:/usr/local/man
```

wobei [Einträge] bestehende Einstellungen sind.

Diese Variablen sollten im gesamten System verwendet werden können. Dies geschieht folgendermaßen:
/etc/login oder /etc/profile.

Wenn Sie ***kein*** Login-Skript haben, müssen Sie die Einträge bei jedem Start Ihres Computers neu setzen.

16.4 Sophos Anti-Virus hat nicht ausreichend Festplattenspeicher

Dieses Problem kann bei der Überprüfung komplexer Archivdateien auftreten.

Wenn Sophos Anti-Virus archivierte Dateien entpackt, speichert es die Ergebnisse im Temp-Verzeichnis. Wenn dieses Verzeichnis relativ klein ist, kann es sein, dass nicht genügend Festplattenspeicher für Sophos Anti-Virus vorhanden ist. Einige Benutzer können auf dasselbe Problem stoßen, wenn Sophos Anti-Virus ihren Festplattenspeicher übersteigt.

Die Lösung besteht darin, entweder das Temp-Verzeichnis zu erweitern oder den Festplattenspeicher zu vergrößern. Sie können aber auch das Verzeichnis ändern, das Sophos Anti-Virus zur Speicherung seiner Ergebnisse verwendet. Dies können Sie mithilfe der Umgebungsvariable SAV_TMP vornehmen.

16.5 Die On-Demand-Überprüfung ist langsam

Ausführliche Überprüfung

Standardmäßig führt Sophos Anti-Virus eine schnelle Überprüfung durch, bei der nur die Bereiche der Dateien geprüft werden, bei denen es wahrscheinlich ist, dass sie Viren enthalten. Ist jedoch die ausführliche Überprüfung aktiviert, so werden alle Bereiche geprüft und die Überprüfung dauert wesentlich länger.

Informieren Sie sich über die -f-Option in Abschnitt 9.6.1.

Eine ausführliche Überprüfung ist bei manchen Viren erforderlich. Sie sollte aber nur von Fall zu Fall gestartet werden (z.B. wenn vom technischen Support von Sophos dazu geraten wurde).

Überprüfung aller Dateien

Standardmäßig überprüft Sophos Anti-Virus nur ausführbare Dateien. Ist Sophos Anti-Virus so konfiguriert, dass alle Dateien überprüft werden, so dauert die Überprüfung entsprechend länger. Wenn neben den ausführbaren Dateien noch andere Erweiterungen überprüft werden sollen, müssen Sie diese zu der Liste an Erweiterungen hinzufügen, die Sophos Anti-Virus als ausführbar bezeichnet.

Siehe -all- und -ext=-Optionen in Abschnitt 9.6.1.

16.6 Archiver sichert alle, im Rahmen der On-Demand-Überprüfung geprüften Dateien

Ihr Archiver erstellt eventuell Backups aller Dateien, die Sophos Anti-Virus im Rahmen der On-Demand-Überprüfung geprüft hat. Dies ist auf die Änderungen zurückzuführen, die Sophos Anti-Virus bei der Zeitmarke Inode Status-Changed Time der Dateien vornimmt.

Nachdem Sophos Anti-Virus eine Datei überprüft hat, setzt es die Zugriffszeit (atime) standardmäßig wieder auf den Zeitpunkt zurück, der vor der Überprüfung angegeben wurde. Dadurch wird jedoch die Zeit Inode Status-Changed Time (ctime) verändert. Verwendet Ihr Archiver die ctime, um festzulegen, ob eine Datei verändert wurde, werden Backups aller von Sophos Anti-Virus überprüften Dateien erstellt.

Um solche Backups zu verhindern, starten Sie den Befehl savscan mit der Option --no-reset-atime.

16.7 Virus/Spyware wurde nicht bereinigt

Wenn Sophos Anti-Virus nicht versucht hat, einen Virus oder Spyware zu bereinigen, prüfen Sie, ob die automatische Bereinigung aktiviert wurde.

Wenn Sophos Anti-Virus den Virus nicht entfernen konnte ('Disinfection failed'), kann es sein, dass es diese Art von Viren nicht entfernen kann.

Sie sollten auch Folgendes überprüfen:

- Handelt es sich um einen Wechseldatenträge (z.B. Diskette oder CD), so stellen Sie sicher, dass er nicht schreibgeschützt ist.
- Wenn sich die Dateien in einem NTFS-Dateisystem befinden, behandeln Sie diese stattdessen auf dem lokalen Computer.

Sophos Anti-Virus bereinigt keine Viren-/Spyware-Fragmente, da es keine Viren/Spyware gefunden hat, die damit genau übereinstimmen. Siehe Abschnitt 16.8.

16.8 Viren-/Spyware-Fragment gemeldet

Wenn ein Viren-/Spyware-Fragment gemeldet wird, aktualisieren Sie Sophos Anti-Virus auf dem betroffenen Computer, damit er über die neuesten Virenkennungsdateien verfügt. Starten Sie dann eine Überprüfung des Computers. Wenn Viren-/Spyware-Fragmente immer noch gemeldet werden, kontaktieren Sie den technischen Support von Sophos.

Die Meldung eines Viren-/Spyware-Fragments deutet darauf hin, dass ein Teil einer Datei mit einem Teil eines Virus oder von Spyware übereinstimmt. Dies kann drei mögliche Ursachen haben:

Variante eines bekannten Virus oder einer bekannter Spyware

Viele neue Viren oder Spyware basieren auf bereits bestehenden Viren oder bestehender Spyware, so dass Code-Fragmente, die für einen bekannten Virus oder bekannte Spyware typisch sind, in neuen Viren oder neuer Spyware erscheinen können. Wenn ein Viren-/Spyware-Fragment gemeldet wird, ist es möglich, dass Sophos Anti-Virus einen neuen Virus oder neue Spyware erkannt hat, der/die aktiv werden könnte.

Beschädigter Virus

Viele Viren enthalten Fehler in ihren Replikationsroutinen, die dazu führen, dass sie Zieldateien inkorrekt infizieren. Ein inaktiver Teil des Virus (möglicherweise ein erheblicher Teil) kann in der HOST-Datei erscheinen und wird von Sophos Anti-Virus entdeckt. Ein beschädigter Virus kann sich nicht verbreiten.

Datenbank, die einen Virus oder Spyware enthält

Bei einer ausführlichen Überprüfung kann Sophos Anti-Virus melden, dass in einer Datenbankdatei ein Viren-/Spyware-Fragment gefunden wurde.

16.9 Fehlermeldung: 'Connection refused' bei Zugriff auf die GUI

Zeigt eine Fehlermeldung an, dass die Verbindung nicht möglich war, wenn Sie versuchen, auf die Sophos Anti-Virus GUI zuzugreifen, kann es daran liegen, dass das Programm Sophos Anti-Virus GUI-Dämon nicht läuft. Um das Programm zu starten, geben Sie Folgendes ein:

```
/etc/init.d/sav-web start
```

16.10 Auf Diskette mit infiziertem Bootsektor kann nicht zugegriffen werden

Standardmäßig verhindert Sophos Anti-Virus den Zugriff auf Wechseldatenträger, deren Bootsektoren infiziert sind. Um den Zugriff zu erlauben (z.B. um Dateien von einer Diskette, die mit einem Bootsektor-Virus infiziert ist, zu kopieren), geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig AllowIfBootSectorThreat enabled
```

Wenn Sie auf die Diskette nicht mehr zugreifen müssen, deaktivieren Sie den Parameter. Entfernen Sie die Diskette aus dem Computer, damit sie nicht versucht, den Computer beim Neustart erneut zu infizieren.

Glossar und Index

Glossar

Ausführbare Dateien: Standardmäßig überprüft Sophos Anti-Virus bei einer On-Demand-Überprüfung nur Dateien, die es als ausführbare Dateien erkennt (auch wenn die ausführliche Überprüfung aktiviert ist). Es ist möglich: Sophos Anti-Virus dazu zu konfigurieren, alle Dateien zu überprüfen, die *Linux* als ausführbar definiert; Sophos Anti-Virus dazu zu konfigurieren, alle Dateien zu überprüfen: und die Liste der Dateien zu ändern, die als ausführbar definiert wurden. Siehe Abschnitt 9.6.1 und 9.6.2.

Ausführliche Überprüfung: Wenn Sophos Anti-Virus konfiguriert ist, eine ausführliche Überprüfung durchzuführen, werden alle Dateien und Teile von Dateien an dem Ort überprüft, der angegeben wurde. Eine ausführliche Überprüfung dauert wesentlich länger als eine schnelle Überprüfung. Mitunter ist eine ausführliche Überprüfung erforderlich, um bestimmte Viren zu entdecken. Siehe Abschnitt 9.6.1.

Bereinigung: Bereinigen ist ein allgemeiner Ausdruck, der Desinfektion und Löschen umfasst.

Bootsektor: Der Teil des Betriebssystems, der zuerst in den Speicher gelesen wird, wenn der Computer eingeschaltet (gebootet) wird. Das in dem Bootsektor gespeicherte Programm wird sodann ausgeführt und lädt den Rest des Betriebssystems von den Systemdateien der CD.

Bootsektor-Virus: Ein Virentyp, der den Anfang des Bootprozesses untergräbt. Ein Bootsektorvirus greift entweder den Master-Bootsektor oder den DOS-Bootsektor an.

CID: Zentrales Installationsverzeichnis; ein zentraler Speicherort in einem Netzwerk, von dem aus Sophos Anti-Virus installiert und aktualisiert wird. Sie müssen für jede Plattform ein unterschiedliches CID erstellen und sicherstellen, dass jedes CID stets up to date ist.

CID-basierte Konfiguration: CID (zentrales Installationsverzeichnis)-basierte Konfiguration, die zuvor Unternehmenskonfiguration genannt wurden, umfasst das Ändern einer Konfigurationsdatei, die im CID gespeichert wird, indem Parametereinträge mit dem Befehl 'savconfig' eingestellt werden. Wenn Endpoints sich dann über das CID aktualisieren, verwenden sie diese Konfiguration.

CID-basierte Konfigurationsdatei: Befindet sich im CID. Speichert die Konfiguration von Sophos Anti-Virus, die auf dem Netzwerk angewandt wird. Normalerweise werden Änderungen an der nicht aktiven Datei vorgenommen, die an einem anderen Ort gespeichert ist und danach werden diese Änderungen mithilfe eines Dienstprogramms in der Live-Datei im CID umgesetzt.

Dämon: Prozess, der im Hintergrund läuft (d.h. unabhängig von jedem Benutzer) ohne Eingabe oder Ausgabe von einem Terminal.

Desinfektion: Bei der Desinfektion wird ein Virus aus einer Datei oder einem Bootsektor entfernt. Die Desinfektion kann jedoch von dem Virus verursachte Änderungen nicht rückgängig machen.

Konsole-basierte Konfiguration: Sie können *Version 6* von Sophos Anti-Virus auf Endpoints mit Sophos Enterprise Console verwalten. Diese läuft nur auf Windows. Sie können damit die meisten Konfigurationen über eine benutzerfreundliche GUI durchführen.

Lokale Konfigurationsdatei: Befindet sich in einem Endpoint. Speichert die Konfiguration von Sophos Anti-Virus, die für diesen Endpoint zutrifft.

Makrovirus: Ein Virentyp, der Makros in einer Windows- oder Mac-Datendatei verwendet, um sich im Speicher auf andere Datendateien verbreiten zu können. Im Gegensatz zu anderen Virentypen sind Makro-Viren bis zu einem gewissen Grad unabhängig von Plattformen.

Master-Bootsektor: Der physikalische Sektor der Festplatte (Sektor 1, Kopf 0, Track 0), der zuerst geladen und ausgeführt wird, wenn der Computer eingeschaltet wird (gebootet wird). Er enthält die Partitionstabelle sowie den Code, um den Bootsektor der 'aktiven' Partition zu laden und auszuführen.

Mount-Point: Punkt in einem Dateisystem, an dem es eine transparente Verknüpfung zu einem oder mehreren Objekten auf einem Dateisystem auf demselben Computer gibt. Siehe auch symbolischer Link.

On-Access-Überprüfung: Fängt Dateien ab, wenn auf sie zugegriffen wird und gestattet Zugriff auf solche, die keine Bedrohung für Ihr Netzwerk darstellen.

On-Demand-Überprüfung: Eine Überprüfung des gesamten oder eines Teils des Computers auf Viren/Spyware, die sofort oder zu einem späteren Zeitpunkt durchgeführt werden kann.

Remoter Mount-Point: Punkt in einem Dateisystem, an dem es eine transparente Verknüpfung zu einem oder mehreren Objekten auf einem Dateisystem auf einem remoten Computer gibt. Siehe auch symbolischer Link.

Schnelle Überprüfung: Der Standard On-Demand-Überprüfungstyp. Sophos Anti-Virus überprüft nur die Bereiche von Dateien, die möglicherweise ausführbaren Code enthalten.

Sophos Anti-Virus Dämon: Kontrolliert die On-Access-Überprüfung und führt die Protokollierung und Benachrichtigung für die On-Access- und On-Demand-Überprüfung durch.

Spyware: Ein Programm, das sich heimlich, durch Täuschung oder Social Engineering auf dem Computer eines Benutzers installiert und Daten von diesem Computer an Dritte ohne Zustimmung oder Wissen des Benutzers sendet. Spyware umfasst Keylogger, Backdoortrojaner, Kennwortdiebstahl und Botnet-Würmer, die den Diebstahl von Unternehmensdaten, finanzielle Verluste und Netzwerkschäden verursachen.

Symbolischer Link: Link zu einer Datei oder einem Verzeichnis auf einem anderen Dateisystem oder einem anderen Computer.

Syslog: Dienstprogramm, das Systemmeldungen (z.B. Meldungen von einem Dämon) protokolliert.

Trojaner: Ein Computerprogramm, das versteckte und schädliche Funktionen ausführt. Normalerweise geben Trojaner vor, eine legitime Funktion zu erfüllen, damit der Benutzer sie ausführt. Backdoortrojaner ermöglichen anderen Benutzern, über das Internet die Steuerung über Ihren Computer zu übernehmen.

Virus: Computerprogramm, das sich über Computer und Netzwerke verbreiten kann, indem es sich an ein Programm (z.B. ein Makro oder einen Bootsektor) anfügt und Kopien von sich erstellt.

Wurm: Ein Virentyp, der kein Überträgerprogramm benötigt, um sich zu vervielfältigen. Würmer vervielfältigen sich selbst und benutzen Kommunikationen zwischen Computern (z.B. E-Mail-Programme), um sich zu verbreiten.

Zentrales Installations-verzeichnis: Siehe CID.

Index

A

Aktualisierung
  Kernel, kundenspezifisch 69
  Kernel, neue Version 69
  Konfigurieren 70
  Sofort 68
Alarm
  Befehlszeile 18, 56
  Desktop Pop-Up 17, 54
  E-Mail 58
Archiv
  On-Access-Überprüfung 40
  On-Demand-Überprüfung 43, 45
Ausführbare Dateien
  UNIX 50
  Windows/DOS 47
Ausführliche Überprüfung 47
Ausschließen von Objekten, On-Access-Überprüfung
  Datei oder Verzeichnis 33
    Zeichenverschlüsselung 38
  Dateisystem
    Dateiüberprüfung 39
Ausschließen von Objekten, On-Demand-Überprüfung
  Datei, Verzeichnis oder Dateisystem 46

B

Beenden der On-Access-Überprüfung 13
Befehlszeile
  Lesen von Argumenten aus Dateien 50
  Übersicht 8
Bildschirmausgaben, in Datei/Gerät kopieren 48
Bootsektor
  infiziert 82
  On-Demand-Überprüfung 15

C

CD Boot-Image 53
CID-basierte Konfiguration 27
Computer, Überprüfung 14

D

Dateisystem, Überprüfung 15
Dateitypen, alle 43
Desinfektion. *Siehe* Entfernen
Durchführen der On-Access-Überprüfung 12
  Automatisch beim Systemstart 11

E

Ebene, bei der Konfiguration 29
Enterprise Console 26
Entfernen
  Informationen erhalten 19
  On-Demand-Überprüfung 21
entfernen
  On-Access-Überprüfung 41
  On-Demand-Überprüfung 46, 48

F

Fehlercodes 16, 46

G

GUI
  konfigurieren 65
  Übersicht 8
  Verbindungsproblem 81

I

infizierter Bootsektor 82

K

Kernel
  angepasst 69
  neue Version 69
Komprimierte Datei 48
Konfiguration eines einzelnen Computers 30
Konfiguration eines Netzwerks 26, 27
Konsole-basierte Konfiguration 26

L

Langsame On-Demand-Überprüfung 79

M

Mailbox 48
Man-Seite wurde nicht gefunden 78
MIME-Datei 47

N

Nachverfolgung
  Aufbewahren von Daten 50
  verhindern 50
Nicht ausreichend Festplattenspeicher 79
Nur Start des Dateisystems, Überprüfung 44

P

Protokoll, Sophos Anti-Virus
  Ansicht 23
  konfigurieren 64

Q

Quarantäne 19, 51

R

Rekursive Überprüfung 48
Remote Computer, Überprüfung 44

S

savconfig, Überblick 30
savsetup, Übersicht 32
Sicherungskopien überprüfter Dateien 80
Spezielle Objekte 52
Spyware
  Analyse 19
  Fragment gemeldet 81
  Nicht entfernt worden 80
Spyware gefunden
  On-Access-Überprüfung 17
  On-Demand-Überprüfung 18
Spyware-Daten
  Speicherort angeben 47
Status der On-Access-Überprüfung 11
Symbolisch verknüpfte Objekte 44, 50

V

Verzeichnis oder Datei, Überprüfung 14
Virendaten
  Speicherort angeben 47
Virus
  Analyse 19
  Fragment gemeldet 81
  Nebeneffekte 22
  Nicht entfernt worden 80
Virus gefunden
  On-Access-Überprüfung 17
  On-Demand-Überprüfung 18

Z

Zeitgesteuerte Überprüfung 98
Zeitpunkt festlegen für Überprüfung 15
Zip-Bombe 48
Zugreifen auf Disketten 82

Technischer Support

Für technischen Support besuchen Sie www.sophos.de/support.

Wenn Sie sich an den technischen Support wenden, halten Sie so viele Informationen wie möglich bereit, darunter:

- Sophos Software-Versionsnummern
- Betriebssysteme und Patch-Level
- Den genauen Wortlaut von Fehlermeldungen

Copyright

Copyright 2005–2010 Sophos Group. All rights reserved. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen von Sophos Plc und Sophos Group. Alle anderen verwendeten Produkt- und Unternehmensnamen sind eingetragene Warenzeichen der jeweiligen Inhaber.

Einige Software-Programme sind für den Benutzer unter der GNU General Public License (GPL) oder ähnlichen freien Software-Lizenzen lizenziert (oder weiterlizenziert), die dem Benutzer u.a. erlauben, bestimmte Programme oder Teile dieser Programme zu kopieren, zu verändern und zu verbreiten sowie den Zugriff auf den Quellcode erlauben. Die GPL erfordert für alle Software-Produkte, die unter der GPL lizenziert sind und an Benutzer in einem ausführbaren binären Format verteilt wird, dass der Quellcode diesen Benutzern ebenfalls zur Verfügung gestellt wird. Für solche Software, die mit diesem Sophos Produkt verteilt wird, steht der Quellcode per Bestellung zur Verfügung, indem eine Anfrage an Sophos gesendet wird:

- E-Mail: savlinuxgpl@sophos.com
- Postanschrift: Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, United Kingdom.

Eine Kopie der GPL-Bestimmungen finden Sie unter www.gnu.org/copyleft/gpl.html

libmagic - file type detection

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994-2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ('PSF'), and the Individual or Organization ('Licensee') accessing and otherwise using this software ('Python') in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to makethe derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa,

this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided "as is" without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

--amk (www.amk.ca)

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL LICENSE

Copyright (c) 1998–2005 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com.

ORIGINAL SSLeay LICENSE

Copyright (c) 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word "cryptographic" can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

TinyXml Xml parser

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Zlib compression tools

(C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

Copyright and licensing information for ACE™, TAO™, CIAO™, and CoSMIC™

ACE[1], TAO[2], CIAO[3], and CoSMIC[4] (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt[5] and his research group[6] at Washington University[7], University of California[8], Irvine, and Vanderbilt University[9], Copyright ©1993–2005, all rights reserved.

Since DOC software is open-source[10], free software, you are free to use, modify, copy, and distribute–perpetually and irrevocably–the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us[11] know so we can promote your project in the DOC software success stories[12].

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies[13] around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE[14], TAO[15], CIAO[16], and CoSMIC[17] web sites are maintained by the DOC Group[18] at the Institute for Software Integrated Systems (ISIS)[19] and the Center for Distributed Object Computing

of Washington University, St. Louis[20] for the development of open-source software as part of the open-source software community[21]. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[22] know.

Douglas C. Schmidt[23]

The ACE home page is http://www.cs.wustl.edu/ACE.html

References

1. http://www.cs.wustl.edu/~schmidt/ACE.html
2. http://www.cs.wustl.edu/~schmidt/TAO.html
3. http://www.dre.vanderbilt.edu/CIAO/
4. http://www.dre.vanderbilt.edu/cosmic/
5. http://www.dre.vanderbilt.edu/~schmidt/
6. http://www.cs.wustl.edu/~schmidt/ACE-members.html
7. http://www.wustl.edu/
8. http://www.uci.edu/
9. http://www.vanderbilt.edu/
10. http://www.the-it-resource.com/Open-Source/Licenses.html
11. mailto:doc_group@cs.wustl.edu
12. http://www.cs.wustl.edu/~schmidt/ACE-users.html
13. http://www.cs.wustl.edu/~schmidt/commercial-support.html
14. http://www.cs.wustl.edu/~schmidt/ACE.html
15. http://www.cs.wustl.edu/~schmidt/TAO.html
16. http://www.dre.vanderbilt.edu/CIAO/
17. http://www.dre.vanderbilt.edu/cosmic/
18. http://www.dre.vanderbilt.edu/
19. http://www.isis.vanderbilt.edu/
20. http://www.cs.wustl.edu/~schmidt/doc-center.html
21. http://www.opensource.org/
22. mailto:d.schmidt@vanderbilt.edu
23. http://www.dre.vanderbilt.edu/~schmidt/

Anhang: Konfigurieren zeitgesteuerter Überprüfungen

Sophos Anti-Virus kann Definitionen mehrerer zeitgesteuerter Überprüfungen speichern.

Hinweis: Auch Enterprise Console oder der Befehl **crontab** ermöglicht Ihnen das Überprüfen von Computern zu festgelegten Zeiten. Weitere Informationen erhalten Sie in der Hilfe zu Enterprise Console und im *Sophos Support-Artikel 12176*. Zeitgesteuerte Überprüfungen, die mit Enterprise Console erstellt wurden, weisen das Präfix „SEC:“ auf und können nur über Enterprise Console geändert oder entfernt werden.

Laden einer zeitgesteuerten Überprüfung aus einer Datei

1. Um eine Vorlagen-Überprüfungsdefinition als Startpunkt zu verwenden, öffnen Sie /opt/sophos-av/doc/namedscan.example.en.

   Um eine neue Überprüfungsdefinition zu erstellen, öffnen Sie eine neue Textdatei.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlage sonstige Optionen fest.

   Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Speichern Sie die Datei in einem beliebigen Verzeichnis. Achten Sie jedoch darauf, dass die Vorlage nicht überschrieben wird.
4. Weisen Sie die über den Befehl **savconfig** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

   Um z.B. eine Überprüfung namens „Daily“ zu laden, die sich unter dem Pfad /home/fred/DailyScan befindet, geben Sie ein:

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily
    /home/fred/DailyScan
   ```

Einrichten einer zeitgesteuerten Überprüfung über Tastatureingabe

1. Weisen Sie die über den Befehl **savconfig** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

   Um zum Beispiel eine Überprüfung namens „Daily“ einzurichten, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily -
   ```

   Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest.

/opt/sophos-av/doc/namedscan.example.en. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste.

Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

Exportieren einer zeitgesteuerten Überprüfung in eine Datei

¶ Wenn Sie über Sophos Anti-Virus eine zeitgesteuerte Überprüfung in eine Datei exportieren möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung und den Pfad der Datei ein, in die Sie die Überprüfung exportieren möchten.

Um z.B. eine Überprüfung namens „Daily“ in die Datei /home/fred/DailyScan zu exportieren, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily >
 /home/fred/DailyScan
```

Exportieren aller zeitgesteuerten Überprüfungen in eine Datei

¶ Wenn Sie alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus in eine Datei exportieren möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Pfad der Datei an, in die die Überprüfungen exportiert werden sollen.

Um z.B. alle zeitgesteuerten Überprüfungen in die Datei /home/fred/AllScans zu exportieren, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans >
 /home/fred/AllScans
```

Hinweis: Die Überprüfung `SEC:FullSystemScan` ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

Senden einer zeitgesteuerten Überprüfung an die Standardausgabe

¶ Wenn Sie eine zeitgesteuerte Überprüfung von Sophos Anti-Virus an die Standardausgabe senden möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

Um zum Beispiel die Definition der Überprüfung „Daily“ an die Standardausgabe zu senden, geben Sie ein:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily
```

Senden aller zeitgesteuerten Überprüfungen an die Standardausgabe

¶ Wenn alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus an die Standardausgabe gesendet werden sollen, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein.

Um alle zeitgesteuerten Überprüfungen an die Standardausgabe zu senden, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig query NamedScans
```

Hinweis: Die Überprüfung `SEC:FullSystemScan` ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

Ändern einer zeitgesteuerten Überprüfung, die aus einer Datei geladen wurde

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Öffnen Sie die Datei, in der die zeitgesteuerte Überprüfung definiert ist, die geändert werden soll.

   Wenn die Überprüfung nicht bereits in einer Datei definiert wurde, können Sie die Überprüfung in eine Datei exportieren. Lesen Sie dazu den Abschnitt *Exportieren einer zeitgesteuerten Überprüfung in eine Datei* auf Seite 23.

2. Passen Sie die Definition ggf. an. Verwenden Sie dabei nur Parameter, die in der Vorlagen-Überprüfungsdefinition aufgeführt sind: /opt/sophos-av/doc/namedscan.example.en. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.
3. Speichern Sie die Datei.
4. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **savconfig** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

   Um z.B. eine Überprüfung namens „Daily“ zu ändern, die sich unter dem Pfad /home/fred/DailyScan befindet, geben Sie ein:

   ```
   /opt/sophos-av/bin/savconfig update NamedScans Daily
    /home/fred/DailyScan
   ```

Ändern einer zeitgesteuerten Überprüfung über Tastatureingabe

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **savconfig** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

   Um zum Beispiel eine Überprüfung namens „Daily“ zu ändern, geben Sie ein:

   ```
   /opt/sophos-av/bin/savconfig update NamedScans Daily -
   ```

   Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest. /opt/sophos-av/doc/namedscan.example.en. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.

   Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

Löschen einer zeitgesteuerten Überprüfung

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

¶ Wenn Sie eine zeitgesteuerte Überprüfung aus Sophos Anti-Virus löschen möchten, geben Sie den Befehl **savconfig** gefolgt vom Vorgang **remove** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

Um zum Beispiel eine Überprüfung namens „Daily“ zu löschen, geben Sie ein:

```
/opt/sophos-av/bin/savconfig remove NamedScans Daily
```

Löschen aller zeitgesteuerten Überprüfungen

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

¶ Geben Sie folgenden Befehl ein, wenn Sie alle zeitgesteuerten Überprüfungen aus Sophos Anti-Virus löschen möchten:

```
/opt/sophos-av/bin/savconfig delete NamedScans
```